

# Controlled Unclassified Information: A Protection or Restriction for Contractors?

By PHILLIP R. SECKMAN, K. TYLER THOMAS, AND JESSICA CHAO



Phillip R. Seckman



K. Tyler Thomas



Jessica Chao

## Introduction

In 2010, President Obama issued Executive Order (EO) 13556, which established the Controlled Unclassified Information (CUI) Program. The CUI Program recognized that nonfederal entities (both state and local governments, contractors, and grant recipients) may receive or generate CUI. Accordingly, the CUI Program contemplates that its requirements will become applicable to these entities via contractual agreements.

For government contractors, particularly Department of Defense (DoD) contractors and their subcontractors, the CUI regulations, 32 C.F.R. Part 2002 (CUI Regulations), have become intertwined with the government's parallel efforts aimed at ensuring that nonfederal information systems that store CUI, or through which CUI is transmitted, have adequate security controls to protect the confidentiality of CUI. In the decade-plus period since the EO was issued, the authors have encountered myriad questions from contractors and subcontractors regarding both the CUI Regulations and the procurement-focused cybersecurity requirements in the Federal Acquisition Regulation (FAR), known as the basic safeguarding rule, and in the Department of Defense Federal Acquisition Regulation Supplement (DFARS), known as the Safeguarding Covered Defense Information and Cyber Incident Reporting rule. Among these questions, two are the focus of this article and primarily relate to the CUI regulation.

The first question concerns how a contractor or subcontractor should go about identifying what, if any, contractor-generated data is CUI and what the contractor

should or can do if its customer will not provide direction or clarity. The second question concerns whether and to what extent marking contractor-generated data as CUI restricts the contractor's right to use the data for its own commercial purposes and to share the data with others. Addressing these questions first requires that we explore the

CUI framework by covering a bit of the history behind the CUI Program, the CUI Regulations, and agency-specific regulations, guidance, and interpretations. The article then turns to some practical considerations relating to these two questions.

In the context of federal government contracting, the CUI Regulations and the cybersecurity rules are quite new. Indeed, we are still awaiting the final FAR rule that will implement National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, and DoD continues its efforts in the context of the Cybersecurity Maturity Model Certification (CMMC) and other initiatives to raise the game across the Defense Industrial Base (DIB) in terms of our collective cybersecurity capability, compliance, and commitment. As the National Archives and Records Administration (NARA), DoD, and other agencies continue to mature the regulatory framework, contractors must perform in the interim, and they are encountering gaps in the regulations, silence in agency guidance, and a government customer that is, sometimes, unhelpful or unwilling to provide clarity. This article aims to provide some practical considerations for counsel supporting their contractor and subcontractor clients and, possibly, perspective for agency counsel to consider when advising agency contracting officers.

## I. The CUI Framework

The nomenclature "CUI" and the CUI Program came into existence in 2010 via EO 13556. Prior to EO 13556, executive agencies employed ad hoc, agency-specific policies, procedures, and markings to safeguard and control various types of unclassified information.<sup>1</sup> Examples of agency-specific designations included "For Official Use Only"/"FOUO," "Sensitive but Unclassified"/"SBU." The differing nomenclatures and the haphazard approach resulted in a patchwork of

---

*Phillip R. Seckman is a partner in the Dentons US LLP government contracts practice and represents clients in government and commercial contract matters. K. Tyler Thomas is a senior managing associate in the Dentons US LLP government contracts practice. Jessica Chao is an associate in the Dentons US LLP government contracts practice.*

systems in which unclassified information that required heightened protection was inconsistently handled, marked, and safeguarded. In fact, a significant policy reason behind EO 13556 was to ease the restrictions on disseminating this information within the federal government to ensure information sharing was occurring while confidentiality of data was being reasonably assured.

EO 13556 sought to remedy this issue and provided consistency and uniformity among executive agencies. Specifically, EO 13556 introduced the nomenclature “CUI,” established the CUI Program, and designated NARA to serve as the executive agent and undertake implementation of the CUI Program. NARA, in turn, through its Information Security Oversight Office (ISSO), published the CUI Regulations in 2016. The CUI Regulations prescribed government-wide implementation standards to increase transparency and consistency in designating, handling, and controlling information that qualifies as CUI.

#### **A. The CUI Regulations Generally**

CUI is an umbrella term 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. However, CUI does not include classified information (see paragraph (e) of this section) or 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.<sup>2</sup>

To further assist in identifying CUI, NARA established a CUI Registry. The CUI Registry is an online repository with organizational index groupings that list authorized categories and subcategories of CUI, their associated approved markings, guidance, policy, and applicable procedures.<sup>3</sup> The law, regulation, or government-wide policy regarding the categories may require or permit safeguarding or dissemination controls in three ways: (i) CUI Basic, (ii) CUI Specified, and (iii) CUI Specified with CUI Basic Controls.<sup>4</sup>

CUI Basic applies when law, regulation, or government-wide policy requires or permits agencies to control or protect the information but provides no specific controls. CUI Specified applies when a law, regulation, or government-wide policy requires or permits agencies to control or protect the information and provides specific controls for doing so. CUI Specified with CUI Basic Controls applies when a law, regulation, or government-wide policy requires or permits agencies to control the information and specifies only some of those controls. Agencies will mark CUI in accordance with the appropriate controls to inform recipients that the information received requires protection.

In addition to marking CUI, accessing and disseminating CUI must occur within the parameters of the relevant authorities to ensure those who receive it continue to maintain the required protections. Pursuant to the CUI Regulations, access of CUI is generally permitted provided that it:

- (i) Abides by the laws, regulations, or Government-wide policies that established the CUI category or subcategory;
- (ii) Furthers a lawful Government purpose;
- (iii) Is not restricted by an authorized limited dissemination control established by the CUI Executive Agent (EA); and,
- (iv) Is not otherwise prohibited by law.<sup>5</sup>

As related to dissemination controls, the CUI Regulations provide that

- (i) Agencies 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.
- (ii) Agencies may not impose controls that unlawfully or improperly restrict access to CUI.<sup>6</sup>

Furthermore, the CUI Registry permits agencies to further limit dissemination for a lawful government purpose, or when required or authorized by relevant law, regulation, or government-wide policy.<sup>7</sup>

#### **B. Agency-Specific Adjustment to, and Interpretation of, the CUI Regulations**

While the CUI Regulations and CUI Registry provide a framework for agencies, agencies are authorized to adopt CUI policies and implement requirements that do not conflict with and are consistent with EO 13556, the CUI Regulations, and the CUI Registry. Accordingly, the DoD implemented the CUI Program requirements by adopting DoD Instruction (DoDI) 5200.48, Controlled Unclassified Information, effective March 6, 2020. DoDI 5200.48 provides policies and procedure for CUI throughout the DoD and establishes the official DoD CUI Registry.<sup>8</sup> DoDI 5200.48 canceled DoD Manual 5200.01, Volume 4, DOD Information Security Program: Controlled Unclassified Information.

Of note, the DoD, through the DoDI, adopted new marking requirements by replacing legacy markings with “CUI” in the banner and footer of the document, as well as portion markings.<sup>9</sup> In addition, the instruction requires the first page or cover of any document containing CUI to include a CUI designation indicator, which must include, at minimum: (i) the name of the DoD Component determining that the information is CUI, if not already indicated on the letterhead or another standard

indicator of origination; (ii) the name of the office making the determination; (iii) a list of the category or categories of CUI in the document; (iv) the distribution or dissemination controls; and (v) the phone number or office mailbox for the originating DoD Component or authorized CUI holder.<sup>10</sup> DoD personnel with access to CUI are required to take a training course that provides further details on marking requirements in addition to additional information regarding compliance and requirements of the CUI Program. The DoDI also designated the Defense Counterintelligence and Security Agency (DCSA) with implementing the CUI Program for the DoD by enumerating eight specific tasks with respect to CUI.<sup>11</sup>

More recently, in October 2021, the National Aeronautics and Space Administration (NASA) incorporated the CUI nomenclature as well, through its release of NASA Procedural Requirement (NPR) 2810.7, Controlled Unclassified Information. To determine compliance with EO 13556, the CUI Regulations, and NPR 2810.7, the NASA HQ, Mission Directorates, Center Directors, and Center Chief Information Security Officers (CISOs) will document compliance through annual self-assessments and reviews conducted by the Office of the Chief Information Officer (OCIO).

Several other agencies have developed similar agency CUI policies that govern their related CUI programs, including the U.S. Department of Energy,<sup>12</sup> the U.S. Department of Agriculture,<sup>13</sup> the U.S. General Services Administration,<sup>14</sup> and the U.S. Department of Commerce.<sup>15</sup>

### **C. Contractors and the CUI Regulations**

The CUI Program is mandatory for federal agencies, not contractors.<sup>16</sup> Contractors, however, are subject to CUI requirements when the requirements are incorporated in a contractual vehicle.<sup>17</sup> For example, a contractor who receives a DoD contract that includes the clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Report, must abide by the CUI requirements given the definition of “Covered defense information.”<sup>18</sup> In addition, contractors, or other nonfederal institutions, need to ensure their information system that processes, stores, or transmits CUI meets the privacy and security requirements provided in NIST SP 800-171.

NASA similarly has a contract clause that requires contractors’ compliance with CUI Regulations. NASA FAR Supplement (NFS) 1852.204-76, Security Requirements for Unclassified Information Technology Resources, provides the relevant security requirements for contractors that store sensitive but unclassified information. In April 2021, NASA released procurement class deviation (PCD) 21-01, which provided a class deviation to revise NFS 1852.204-76 to implement the CUI Program—Security Requirements for Unclassified Information Technology Resources (Deviation 21-01). This deviation provided that the clause is applicable to all NASA contractors and subcontractors that stored, managed,

processed, or accessed sensitive but unclassified information or CUI. As noted above, NASA released NPR 2810.7, which incorporated CUI and made clear sensitive but unclassified information (SBU) would no longer be used beyond legacy markings, including reusing the marking on new documents that are derived from marked legacy information.

As of the drafting of this article, there are various open FAR cases addressing cybersecurity requirements including FAR Case 2017-016 (Controlled Unclassified Information) and FAR Case 2021-019 (Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems). FAR Case 2017-016, in pertinent part, seeks to implement the NARA CUI Program.<sup>19</sup> On February 24, 2022, the Civilian Agency Acquisition Council Chair sent the draft proposed FAR rule to the Office of Information and Regulatory Affairs for review. FAR Case 2021-019 addresses sections 2(i) and 8(b) of EO 14028, Improving the Nation’s Cybersecurity, issued on May 12, 2021. Section 2(i) of EO 14028 provides that within 60 days of the EO:

[T]he Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Defense acting through the Director of the NSA, the Director of OMB, and the Administrator of General Services, shall review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements. Such recommendations shall include consideration of the scope of contractors and associated service providers to be covered by the proposed contract language.<sup>20</sup>

Section 8(b) states:

Within 14 days of the date of this order, the Secretary of Homeland Security, in consultation with the Attorney General and the Administrator of the Office of Electronic Government within OMB, shall provide to the Director of OMB recommendations on requirements for logging events and retaining other relevant data within an agency’s systems and networks.<sup>21</sup>

This FAR case seeks to standardize cybersecurity contractual requirements for unclassified federal information systems pursuant to sections 2(i) and 8(b) of EO 14028. In addition to these FAR cases, DoD is in the process of establishing the CMMC, version 2.0, which will be codified through rulemaking. CMMC 2.0 will not become a contractual requirement until the rulemaking process is complete, and while the proposed rule has not yet been published for public comment, DoD anticipates the process to take between nine and 24 months.

To comply with current contract requirements, and to prepare for upcoming FAR and DFARS rules, it is imperative contractors understand CUI and maintain

practices to comply with the CUI Regulations from marking through decontrol if they possess or anticipate possessing CUI. The remainder of this article discusses a couple of practical considerations that frequently arise as contractors familiarize themselves with CUI and CUI requirements flowed to them in contracts.

## II. Practical Considerations for Contractors

A contractor's understanding of CUI and the CUI Regulations (and when the CUI Regulations apply to a contractor) is the tip of the iceberg. As we are still relatively early in the adoption of the CUI framework, many uncertainties regarding CUI remain. Two recurrent issues that have arisen in our experience include (a) identifying throughout contract performance what, if any, contractor-generated data is CUI and (b) understanding the ability of a contractor to share its own data that is marked as CUI. Practical considerations related to each of these two issues are discussed, in turn, below.

### A. Overcoming Difficulties in Identifying Whether Data Generated During Contract Performance Is CUI

As identified above, CUI requirements become applicable to contractors through their contracts; the CUI Regulations do not directly apply to contractors. The government (or higher-tier contractor depending on where a company falls within the supply chain) should identify which data provided to a contractor (or subcontractor) under a contract is CUI.<sup>22</sup> While adjusting to the CUI framework has taken some time, agencies are increasingly identifying and marking CUI prior to providing it to contractors. This often is not an area of concern for contractors.

Instead, one difficulty for contractors that often arises relates to data the contractor is generating. Specifically, what generated data does the government consider to be CUI that must be marked as such? Relevant guidance identifies that the government is the party responsible for determining when the contractor is required to mark specific contractor-generated data as CUI, and also is responsible for placing such requirements in the contract.<sup>23</sup> Thus far, unfortunately, contracts seldom identify clearly, or at all, the contractor-generated data that is to be marked as CUI, when it is to be marked, and whether the marking is also to be applied only to delivered final versions or also to drafts.

When requesting guidance from customers, some contractors are being informed that they should treat everything as CUI, while others receive no response and no guidance whatsoever. The more common scenario is a lack of guidance being provided to contractors, but it is noteworthy that an approach of marking "everything" as CUI should be taken with caution as overmarking data with CUI legends also might be considered misuse of CUI.<sup>24</sup>

In the face of the lack of meaningful guidance, contractors may take a variety of actions to reduce risk of noncompliance with CUI requirements. First, it is advisable that contractors adopt an internal policy or

procedure that is consistent with the CUI Regulations and provides a company-specific approach to complying with CUI requirements. A few key components of such a policy or procedure may include:

- promoting handling, safeguarding, and dissemination of marked CUI in accordance with CUI Regulations, as well as applicable contractual requirements;
- identifying the means through which electronic transmission of CUI is permitted;
- establishing a framework for the management of received CUI, such that the systems on which CUI resides can be readily identified;
- requiring use of standard protective markings appropriate for internal proprietary/sensitive documentation in accordance with company procedures for the protection of such proprietary materials in advance of any such company-generated data being identified or marked as CUI (to otherwise promote protection and reduce dissemination of such company data);
- providing an approach to seek clarification when CUI identification and marking requirements are unclear, such as:
  - identifying the internal point of contact for questions;
  - requiring that the point of contact attempt to seek clarification from customers, when necessary; and
  - establishing a uniform approach that will be followed when clarification is not received or until clarification is received. Three scenarios to consider in order to promote clarity in the adopted approach include establishing how the company will handle:
    - company-generated data that is not required to be delivered to the customer under the contract (i.e., should the company not mark it as CUI but still require marking of the data with company proprietary legends?);
    - company-generated data that is delivered to the customer under the contract (i.e., should the company only mark data delivered to the customer as CUI when either (a) the deliverable incorporates other data previously marked as CUI or (b) the contract identifies (such as through a Contract Data Requirements List) that a given deliverable is CUI?);
    - company-generated data that supports deliverables to the government that are marked as CUI (i.e., should the company only mark the specific deliverable as CUI and not contractor-generated data that remains on the contractor's systems and is not an express part of that deliverable?).

Importantly, the adopted policies and procedures



should be constructed specific to the contractor to promote compliance for that contractor; there is no “one size fits all” approach. Additionally, such a policy or procedure need not be limited to CUI but could be more broadly constructed to promote compliance with applicable government contract cybersecurity requirements. In any case, any CUI policy or procedure should be drafted with due consideration to any related obligations under DFARS 252.204-7012 and a contractor’s system security plan.

Second, when a contractor is instructed either that all data is CUI or is not provided guidance from its customer as to what data that the contractor generates is to be considered CUI, then it is advisable that the contractor adopt a uniform approach (consistent with its policy or procedure, or otherwise its adopted practice) and inform the customer of such approach, as the customer may not have access to the contractor’s internal policies and procedures. This notice could be prepared in advance and provided in a form letter that is updated per contract. This approach seeks to mitigate risk to the contractor by placing the customer on notice of the reasonable approach taken in the face of uncertainty or ambiguity in the contract. This approach also provides the customer with the opportunity to take issue with the approach, which can then serve as a means of more productively, and proactively, resolving areas of disagreement.

Third, it is possible for an issue to arise in which a contractor receives data marked as CUI that should not be so marked or the government marks (or directs a contractor to mark) contractor-generated data as CUI that a contractor disagrees should be so marked. When such a circumstance arises, then it is important for contractors to continue to abide by the markings until they are removed.<sup>25</sup>

Well-constructed policies and procedures, followed by letters to customers (when needed), have proven successful for some contractors in the authors’ experience. These communications can serve either as a means for gaining clarity from customers or at least clearly documenting the contractor’s approach to managing its CUI program. This clarity is important in minimizing the risk of mishandling CUI because, unsurprisingly, the first step in appropriately safeguarding CUI is understanding what data in a contractor’s possession is CUI in the first place. An approach of not overmarking data as CUI also is a consideration to reduce risk.

### ***B. Understanding a Contractor’s Ability to Share Its Own Data Marked as CUI***

A frequent, and understandable, concern among many contractors is the impact that marking their data as CUI may have on their ability to subsequently share that data with third parties or otherwise make commercial use of that data. In determining the ability to share and use contractor-owned CUI, contractors must hone in on the relevant underlying law, regulation, or government-wide policy for why such data is marked as CUI, rather than focusing solely on the fact the data is considered to be

“CUI.” Statedly differently, the CUI designation (specifically if it is CUI Specific) may provide some insight into the dissemination and use restriction imposed by another law, regulation, or contract provision. And it is that underlying restriction (rather than the CUI Regulations) that typically best informs and defines the contractor’s ability to commercially use or share contractor-owned data.

As a starting point, it is important to reemphasize that CUI is data that is created or possessed for or on behalf of the government.<sup>26</sup> It does not include “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.”<sup>27</sup> Thus, when a contractor generates data itself and that data was not created for or on behalf of the government, it does not constitute CUI. This removes such contractor self-generated data from the purview of the CUI Regulations and avoids the restrictions of dissemination. This does not, however, eliminate the possibility of other types of restrictions beyond the CUI Regulations that could potentially be imposed upon such contractor self-generated data and the need to consider and comply with such other restrictions (e.g., export control laws). Subject to compliance with such limitations, however, the contractor is free to use the data for its commercial purposes and share it with third parties as it deems appropriate.

As related to contractor-owned data that does constitute CUI and is marked as such, the dissemination restrictions on such data appear less clear, but ultimately should result in a similar end point to non-CUI. Specifically, while the CUI designation should signal to contractors that there likely is an underlying restriction that must be reviewed to determine the permitted dissemination of such data, it is not the CUI Regulation but rather that underlying restriction resulting in the CUI designation that controls the commercial use and dissemination of the contractor-owned data marked as CUI. This is because the three CUI types (CUI Basic, CUI Specified, and CUI Specified with CUI Basic Controls) apply when law, regulation, or government-wide policy requires or permits agencies to control or protect the information.<sup>28</sup> This means that CUI and the CUI Regulations fundamentally build upon other laws, regulations, or government-wide policies that govern whether any particular type of data is CUI, and the applicable restrictions. Consequently, at the crux of the matter, contractors must determine whether there is a law, regulation, or government-wide policy (beyond the CUI Regulation) that governs, and if so, what level of protection or control over the dissemination of the data is contained therein.

An ambiguity that may be encountered is in the context of circumstances where dissemination is not addressed in such underlying law, regulation, or government-wide policy. In such a circumstance, the CUI Regulations provide a gap filler to limit dissemination. In

that scenario, dissemination of CUI, again, is generally permitted provided that it:

- (i) Abides by the laws, regulations, or Government-wide policies that established the CUI category or subcategory;
- (ii) Furthers a lawful Government purpose;
- (iii) Is not restricted by an authorized limited dissemination control established by the CUI EA; and,
- (iv) Is not otherwise prohibited by law.<sup>29</sup>

In this circumstance, we are assuming (i) and (iii) do not restrict the contemplated dissemination and that the dissemination, in accordance with (iv), would not violate law, such that the only potential restriction remaining would be whether the dissemination furthers a lawful government purpose. It may seem strange that a contractor's primary inquiry as to whether dissemination of data that it owns is permitted should be dependent on whether doing so would "further a lawful Government purpose."<sup>30</sup> That said, the definition of what furthering a lawful government purpose means provides an avenue for a contractor to do just that. Furthering a lawful government purpose means furthering "any activity, mission, function, operation or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement)."<sup>31</sup>

A contractor disseminating its own data for lawful commercial purposes, when not otherwise prohibited by law, should be viewed as conduct that furthers a lawful government purpose. This is because contractors generally retain ownership of contractor-generated data.<sup>32</sup> The regulatory framework of a contractor retaining ownership and only granting the government license rights in such data is meant to provide an incentive for contractors to conduct business with and perform government contracts, as well as to commercialize that data to strengthen the economy. In fact, the Bayh-Dole Act, which similarly is geared toward providing incentives for contractors to retain title to patents and then use such ownership rights commercially, exemplifies how government contractors are motivated to use their innovations created under government contracts to strengthen the U.S. industrial base and the U.S. economy generally.<sup>33</sup> Thus, the commercial use of a contractor's own data that may be marked as CUI but is not subject to any specific limited dissemination by an underlying law, regulation, or government-wide policy arguably constitutes an activity recognized by the U.S. government as within the scope of a contractor's legal authorities.

This conclusion is supported by the fact that it would be unreasonable to interpret the "lawful government purpose" inquiry to result in a circumstance where the dissemination of CUI Basic data would be more


restrictive than CUI Specified.<sup>34</sup> It also is supported by the purpose of the CUI Regulations not being to overly restrict the dissemination of CUI.<sup>35</sup> Moreover, the regulatory history supports a conclusion that NARA's intent was not to restrict a contractor's use of its own data, but instead to provide protections to the benefit of the contractor once the data is provided to the government. Specifically, in response to comments asserting that the safeguarding requirements and NIST SP 800-171 are too extreme and burdensome, NARA responded that its focus was on protecting the "great deal of information [the government receives] from individuals, businesses, and other entities that it is required to protect."<sup>36</sup> Relatedly, a NARA CUI Program analyst has explained that when a contractor releases proprietary information to the government, the government would appropriately mark that information and protect it as CUI.<sup>37</sup> If the contractor subsequently received the same proprietary information it shared with the government back, but now with a CUI marking, the proprietary information would not be CUI to the contractor *unless* the government had purchased the contractor's rights in the information.<sup>38</sup>

This regulatory history clarifies that the focus of the protection relates to when the government provides data outside the government (e.g., when the government disseminates one contractor's data to another contractor). For example, when data is CUI because it is "General Proprietary Business Information" of a contractor, it is logical that when the government provides Contractor A's information to Contractor B, such as based on Government Purpose Rights, that the government would limit Contractor B's further dissemination of that "General Proprietary Business Information" to a government purpose. It also is possible, however, that Contractor B could receive that same data directly from Contractor A (and outside of government involvement) and be permitted to use it beyond a government purpose. This leads to the reasonable conclusion that if data is marked CUI because it is "General Proprietary Business Information" of Contractor A, then Contractor A may continue to use its own data and share it with third parties regardless of whether such sharing furthers "a lawful government purpose," as that phrase is used in the CUI Regulations.

Overall, the CUI Program and CUI Regulations should not reasonably be construed to restrict a contractor's right to use, release, or share its own data by commercializing it, even after marking it as CUI, absent a dissemination restriction by another law, regulation, or contractual provision. And the marking of data as CUI likewise should not affect a contractor's right in its own data absent the contractor providing such rights via another contractual clause or otherwise.<sup>39</sup>

### III. Conclusion

This article explains how contractors and subcontractors can work with their government or higher-tier customers to clearly identify what is and what is not CUI under

their contracts. When a government or higher-tier customer is not communicative, cooperative, or willing to commit on this subject, however, we explore various strategies to enable a contractor to move forward with contract performance by clearly communicating the approach to CUI compliance. This article also explores why contractors generating data that they own, which may incidentally be marked as CUI when delivered to the government or a higher-tier contractor, remain free to use that data for commercial purposes and may share that data with third parties provided doing so is not otherwise prohibited by law. While the conclusion we reach on this subject has not, as far as we are aware, been addressed by a court, we think it is the most reasonable interpretation of the CUI regulation. 

## Endnotes

1. See Exec. Order No. 13556, 75 Fed. Reg. 68,675 (Nov. 9, 2010).
2. 32 C.F.R. § 2002.4(h).
3. *Id.* § 2002.4(p); see also *CUI Registry*, NAT'L ARCHIVES, <https://www.archives.gov/cui/registry/category-list>.
4. 32 C.F.R. § 2002.4(p).
5. *Id.* § 2002.16(a)(1).
6. *Id.* § 2002.16(a)(2).
7. Examples of limited dissemination controls include attorney work product (Attorney-WP), attorney-client (Attorney-Client), dissemination list controlled (DL ONLY), federal employees and contractors only (FEDCON), federal employees only (FED ONLY), no dissemination to contractors (NOCON), no foreign dissemination (NOFORN), and releasable by information disclosure official (RELIDO). *CUI Registry: Limited Dissemination Controls*, NAT'L ARCHIVES, <https://www.archives.gov/cui/registry/limited-dissemination>.
8. U.S. DEP'T OF DEF., DoD INSTRUCTION 5200.48, CONTROLLED UNCLASSIFIED INFORMATION (CUI) (Mar. 6, 2020).
9. *Id.* § 3.4.
10. *Id.* § 3.4(f).
11. *Id.* § 2.3.
12. U.S. DEP'T OF ENERGY, DOE O 205.1C, DEPARTMENT OF ENERGY CYBERSECURITY PROGRAM (May 15, 2019).
13. U.S. DEP'T OF AGRIC., DR 3440-003, CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM (Sept. 13, 2021).
14. GEN. SERV. ADMIN., CIO 2103.2, CONTROLLED UNCLASSIFIED INFORMATION (CUI) POLICY (Apr. 10, 2021).
15. U.S. DEP'T OF COM., OPBM-NP-18-0001, CONTROLLED UNCLASSIFIED INFORMATION (CUI) GUIDELINES (Aug. 2019).
16. 32 C.F.R. § 2002.1(f).
17. *Id.*; see also *id.* §§ 2002.4(c), 2002.16(a)(5) & (6).
18. "'Covered defense information' means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." DFARS 252.204-7012.
19. FAR Case 2017-016 also seeks to implement the Office of Management and Budget Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information. This memorandum provides guidance and policy for

agencies to prepare for and respond to a breach of personally identifiable information.

20. Exec. Order No. 14028, 86 Fed. Reg. 26,633, 26,635 (May 17, 2021).

21. *Id.* at 26,644.

22. 32 C.F.R. § 2002.4(h).

23. See, e.g., DoDI 5200.48, *supra* note 8 (sections 5.3, providing that CUI requirements "will be articulated in the contract, grant, or other legal agreement, as appropriate," and 3.4.f, requiring information marked CUI to include the DoD component "determining that the information is CUI"); Cwllace, *CUI Marking Class Q&A (from May 19)*, NAT'L ARCHIVES: CUI PROGRAM BLOG (July 9, 2020), <https://isoo.blogs.archives.gov/2020/07/09/cui-marking-class-qa-from-may-19/> ("Question: For Industry Contractors, do we ever mark CUI? Answer: Yes, but only when instructed to do so in the contract or supporting documentation."). The guidance further identifies that the government should clarify what, if any, data should be marked as CUI. See *id.* ("Questions regarding the status of information (marked or unmarked) should be directed back to the contracting activity.").

24. See 32 C.F.R. § 2002.4(ee) (defining "misuse of CUI" as "includ[ing] designating or marking information as CUI when it does not qualify as CUI").

25. See, e.g., *id.* § 2002.52; DoDI 5200.48 § 3.5(a)(6).

26. 32 C.F.R. § 2002.4(h).

27. *Id.*

28. *Id.*

29. *Id.* § 2002.16(a)(1).

30. *Id.*

31. *Id.* § 2002.4(bb) (emphasis added).

32. For example, the DFARS clauses expressly provide contractors with the ability to assign or grant rights in its data. See DFARS 252.227-7013.

33. 35 U.S.C. § 200 (identifying the statute's policy and objective).

34. See 32 C.F.R. § 2002.16(b)(2)(ii) ("In the absence of specific dissemination restrictions in the authorizing law, regulation, or Government-wide policy, agencies may disseminate CUI Specified as they would CUI Basic.").

35. See *id.*; see also *Food & Drug Admin. v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000) ("[C]ourts must therefore interpret the statute as a symmetrical and coherent regulatory scheme and fit, if possible, all parts into an harmonious whole." (Citation omitted.)).

36. Controlled Unclassified Information, 81 Fed. Reg. 63,323, 63,325 (Sept. 14, 2016) ("It would be nonsensical to require the Government to protect and control information but to simultaneously allow others to leave the same information unprotected.").

37. See Devincaseycui, *A Short Video Talking About CUI and the Contracting Environment: stackArmor Micro Summit on NIST 800-171—Devin Casey*, NAT'L ARCHIVES: CUI PROGRAM BLOG (Mar. 22, 2018), <https://isoo.blogs.archives.gov/2018/03/22/a-short-video-talking-about-cui-and-the-contracting-environment/>.

38. See *id.* at 13:18-14:35.

39. This interpretation is not free from risk. The government could argue that the CUI in support of the performance of the contract must be limited to dissemination only when related to furthering a government purpose and such government purpose must be limited to government application. This approach would ignore the language of the CUI Regulations and regulatory purpose. It would also ignore the rationale behind contractors retaining ownership of data developed with government funding. While the CUI may have supported the performance of the contract, despite the government involvement, CUI that is contractor-generated and owned data logically do not become government-owned nor can they be limited to furthering a government purpose absent a law, regulation, or other agreement stating otherwise.