COVINGTON

NARA Sets the Stage for a Final FAR Cyber Clause

September 19, 2016

Government Contracts

On September 14, 2016, the National Archives and Record Administration (NARA) issued the "Controlled Unclassified Information Final Rule" (Final Rule), effective November 13, 2016, establishing consistent practices and procedures for safeguarding, disseminating, controlling, destroying, and marking Controlled Unclassified Information (CUI) across Executive Branch departments and agencies. Although the Final Rule only applies directly to "executive branch agencies that designate or handle information that meets the standards for CUI," it also applies indirectly to non-executive branch entities "through incorporation into agreements."[1] These non-executive branch entities include contractors whose agreements will likely be impacted by these requirements in the near future.[2] Accordingly, contractors must be aware of the new rule's requirements. Furthermore, the release of this Final Rule now paves the way for a final FAR clause that will impose contractor safeguarding requirements (and potentially cyber incident reporting requirements) across the government.

Background

On November 4, 2010, President Obama signed Executive Order 13556 (CUI EO) to establish a uniform approach across agencies for managing unclassified information that requires safeguarding or dissemination controls.[3] The goal of the CUI EO was to address the previously ad hoc, agency-specific approach to safeguarding and managing such information, which had on occasion resulted in agencies mishandling information and had often impeded information sharing. The CUI EO assigned NARA with responsibility, in consultation with various agencies, to review agency input and approve uniform CUI classifications and associated markings, and issue any directives necessary to implement the CUI EO.

The first step in NARA's efforts was the establishment of the CUI Registry. Developed in consultation with more than 150 government entities, this registry lists 23 categories and 84 subcategories of information that are considered CUI. These categories include, among others, copyright and patent information, controlled technical information, personally identifiable information, raw census data, intelligence and law enforcement data, and information systems vulnerabilities.

The recently issued Final Rule is the next major step in NARA's efforts to create a uniform system for safeguarding and managing CUI, including the establishment of standardized rules for how CUI must be handled by executive agencies, as well as those entities receiving CUI from executive agencies.

---

[1] 32 C.F.R. § 2002.1(f).
[2] 32 C.F.R. § 2002.4(c) and 2002.12.
[3] EO No. 13556 (Nov. 9, 2010).

Highlights from the Final Rule

The Final Rule includes several key elements:

- Definition of CUI: The Final Rule defines CUI 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."[4] This means that information will qualify as CUI if a law, regulation, or government-wide policy either requires that agencies exercise safeguarding or dissemination controls over specific information or permits agencies the discretion to exercise such control.[5] This definition is quite broad and is in keeping with the similarly broad definition of Covered Defense Information (CDI) formulated by DoD in its network penetration and safeguarding rule—DFARS 252.204-7012.
- The CUI Registry: The Final Rule reinforces the importance of the CUI Registry, identifying it as the repository for information, guidance, policy, and requirements for handling CUI.[6] The registry designates what level of control is required for a given category of CUI and includes citations to laws, regulations, and/or government-wide policies that form the basis for each category and subcategory. For example, for "controlled technical information," the CUI Registry cites to DFARS 252.204-7012. An excerpt of the CUI Registry entry for Controlled Technical Information is set forth below[7]:

CUI Registry

Controlled Technical Information

Category-Subcategory:	**Controlled Technical Information**
Category Description:	Controlled Technical Information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with Department of Defense Instruction 5230.24, "Distribution Statements of Technical Documents." The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
Subcategory Description:	N/A
Marking:	PLACEHOLDER

- **CUI Specified authorities include specific handling practices that differ from general CUI requirements. For Specified authorities, reference individual Safeguarding/Dissemination control citations for distinct requirements**
- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizin the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
48 CFR 252.204-7012	Specified	

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations, and the CUI Registry maintenance schedule.

[4] 32 C.F.R. § 2002.4(h).
[5] 32 C.F.R. § 2002.4(nn).
[6] 32 C.F.R. § 2010.
[7] See https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html

- CUI Categories and Subcategories: Under the Final Rule, the CUI Registry categories and subcategories are the exclusive means of designating CUI throughout the executive branch.[8] Changes to these categories and subcategories must be approved by the CUI Executive Agent (NARA).[9]
- Safeguarding: The Final Rule provides that agencies "must safeguard CUI at all times in a manner that minimizes the risk of unauthorized disclosure while allowing timely access by authorized holders."[10] Different safeguarding obligations will apply if the CUI at issue is CUI Basic or CUI Specified. "CUI Specified" is the subset of CUI where there are specific rules, regulations, and/or laws that specify safeguarding requirements.[11] For example, technical controlled information noted above is designated as CUI Specified, which must be protected consistent with the requirements imposed by DFARS 252.204-7012.

  "CUI Basic" is the "subset of CUI where the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls."[12] An example of CUI Basic data is that related to law enforcement informants. The CUI Registry entry for this type of CUI is set forth below.[13] Because it is designated "basic," this means that the authorizing statutes and regulations for these types of data do not specify particular handling or dissemination controls.

CUI Registry

Law Enforcement-Informant

Category-Subcategory:	**Law Enforcement-Informant**
Category Description:	Related to techniques and procedures for law enforcement operations, investigations, prosecutions, or enforcement actions.
Subcategory Description:	Related to the identity of a human source.
Marking:	PLACEHOLDER

- Whether CUI is Basic or Specified is determined by the applicable Safeguarding and/or Dissemination Authority for that CUI.
- Each "Safeguarding and/or Dissemination Authority" citation links to the statute, regulation or government-wide policy authorizing the control of that information as CUI.
- Each "Sanctions" authority links to the statute, regulation or government-wide policy that includes penalties for CUI misuse of CUI for the associated "Safeguarding and/or Dissemination Authority" on the same line.

Safeguarding and/or Dissemination Authority	Basic or Specified	Sanctions
5 CFR 736.103	Basic	
21 CFR 20.64(a)(4)	Basic	
10 CFR 19.16(a)	Basic	

Authority links are updated based on regular re-publication of the United States Code and Code of Federal Regulations, and the CUI Registry maintenance schedule.

[8] 32 C.F.R. § 2002.12.
[9] Thus, it is possible that the DFARS Rule will be amended to make the definitions of CDI consistent with the FAR Rule's definition of CUI.
[10] 32 C.F.R. § 2002.14(a).
[11] 32 C.F.R. § 2002.4(r).
[12] 32 C.F.R. § 2002.4(j).
[13] See https://www.archives.gov/cui/registry/category-detail/law-enforcement-informant.html

When CUI is processed, stored, or transmitted on an information system, the level of safeguarding protections that agencies must comply with will depend on whether the information system is one operated on behalf of the government or if the information system is a non-federal entity's information system that stores, processes, or transmits CUI. For the former, information systems operated on behalf of the government "are subject to the requirements of this part as though they are the agency's systems," including any additional requirements that the agency imposes on its own systems.[14] For non-federal entity information systems with CUI, such as a contractor's internal systems, the agency can only impose 800-171 security controls, unless the statute, regulations, or government-wide policy imposes a more stringent requirement for the type of CUI at issue.[15] Thus, unless contractors have segregated systems per type of CUI, the safeguarding obligations for a network are likely going to be dictated by the type of CUI with the most stringent protection requirements.

The Final Rule also provides specific requirements for protecting CUI outside of information systems, such as when under the physical control of an authorized user and provides direction on how to protect CUI when shipping or mailing; when storing CUI in a physical space (hard copy CUI); when reproducing CUI; and when destroying CUI.

- Accessing and Disseminating: The Final Rule sets forth procedures for agencies to disseminate and permit access to CUI. Agencies are directed to appropriately mark any CUI prior to disseminating within the government and agencies are encouraged to enter into agreements before disseminating CUI to non-federal entities. Minimum requirements for such agreements are that the non-federal entity must (1) handle CUI in accordance with the executive order, the Final Rule, and the CUI Registry; (2) agree that any misuse of CUI is subject to applicable laws, regulations, and government-wide policies; and (3) report any non-compliance with handling requirements to the disseminating agency.[16] This self-reporting requirement is one that contractors should expect to see in contracts after November 2016. It would cover both intentional and unintentional disclosure of UCI, as well as errors in the safeguarding of UCI.[17]
- Decontrolling: The Final Rule establishes procedures for agencies to decontrol CUI.[18] Decontrolling CUI will relieve authorized holders from requirements to handle the information under the CUI rule, but it does not equate to authorization for public release of the information.[19]
- Marking: Only those markings listed in the CUI Registry are authorized for use on unclassified information requiring safeguarding or dissemination controls.[20] The Final Rule provides that the CUI control marking may consist of either the word "CONTROLLED" or the acronym "CUI," and that an agency must specify one of the

[14] 32 C.F.R. § 2002.14(h)(1).
[15] 32 C.F.R. § 2002.14(h)(2).
[16] 32 C.F.R. § 2002.16(a)(6).
[17] *See* 32 C.F.R. § 2002.4(ee) (defining the "Misuse of CUI" to include "intentional violations or unintentional errors in safeguarding or disseminating CUI").
[18] 32 C.F.R. § 2002.18.
[19] 32 C.F.R. § 2002.18(e).
[20] 32 C.F.R. § 2002.20.

other.[21] The Final Rule explicitly prohibits agencies from modifying or deviating from the method of use prescribed for marking unless approved by NARA.[22]

The Final Rule recognizes that it may not be practical to individually re-mark legacy materials and allows agencies to use "alternative permitted marking method."[23] The Final Rule does not provide significant guidance on what qualifies as an appropriate alternative method other than to state that when it is "impractical" for an agency to mark each legacy piece of information, the agency must use an alternate approach that is "readily apparent (for example through user access agreements, a computer system digital splash screen (e.g., alerts that flash up when accessing the systems), or signs in storage areas or contains."[24]

- Waivers: The Final Rule includes a waiver provision on marking if the need to mark is "excessively burdensome" or if there are "exigent circumstances."[25] The approval for the waiver must come from the senior agency official charged with oversight for CUI—the CUI SAO.[26]
- FOIA Implications: The Final Rule notes that not every release of information under the Freedom of Information Act will qualify as a public released and the Final Rule states that the agency may still need to control the CUI unless the agency decontrols the information.[27] Thus, it appears that a contractor could still be subject to CUI control for information that has been released to a third party pursuant to a FOIA request.

Implications for Government Contractors

This Final Rule is almost five years in the making. The inconsistencies within the government in defining how information should be classified has been a significant obstacle to effective cybersecurity protection because there has been no common baseline for defining what information requires which levels of controls. Based on this Final Rule, contractors should expect to see a final FAR Rule that imposes safeguarding requirements for CUI in the non-DoD arena, as well as possibly reporting requirements for cyber incidents outside of DoD contracts. It appears that the security controls that will be imposed on internal contractor systems will mirror that of DoD's requirements for compliance with the NIST 800-171 controls. However, while DoD contractors have until December 31, 2017 to fully comply with those requirements, it is unclear if the expected FAR Rule will allow for a similar implementation period.

[21] 32 C.F.R. § 2002.20(b)(1). As of September 16, 2016, the CUI Registry is still listing "PLACEHOLDER" for markings.
[22] 32 C.F.R. § 2002.20(b)(1)(iii).
[23] 32 C.F.R. § 2002.20(a)(8).
[24] *Id*.
[25] 32 C.F.R. § 2002.38(a) and (c).
[26] 32 C.F.R. § 2002.38(b).
[27] 32 C.F.R. §2002.44.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Government Contracts practice:

Patrick Stanton	+1 202 662 5441	pstanton@cov.com
Susan Cassidy	+1 202 662 5348	scassidy@cov.com