IT Alliance for Public Sector
A Division of ITI

Federal Actions to Enable Contractors to Protect "Covered Defense Information" and "Controlled Unclassified Information"

A White Paper Published in Conjunction with the IT Alliance for Public Sector[1]

March 27, 2017

Prepared by ITAPS Associate Member:

Robert S. Metzger, Shareholder
ROGERS JOSEPH O'DONNELL, a Professional Law Corporation
Washington, DC 20005
rmetzger@rjo.com | 202-777-8951

For comments or questions, please contact:

Pamela Walker
Senior Director, Federal Public Sector Technology
pwalker@itic.org | 202-626-5775

[1] **About ITAPS**. ITAPS, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies building and integrating the latest innovative technologies for the public sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more. Follow us on Twitter @ITAlliancePS.

Executive Summary

Over the past six months, important actions have been taken by the federal government to safeguard the confidentiality of information that the government provides to or receives from its suppliers. The key actions are the Final Rule, "Controlled Unclassified Information" (CUI), published on September 14, 2016; the revised (and final) DFARS rule, "Network Penetration Reporting and Contracting For Cloud Services", of October 21, 2016, and Revision 1 to NIST SP 800-171 ("Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"). A recent development, also focused on CUI, was the publication on January 19, 2017, of the DHS Proposed Rule, "Homeland Security Acquisition Regulation (HSAR); Safeguarding of Controlled Unclassified Information."

These actions (excepting the DHS Proposed HSAR) establish the process by which agencies designate federal information which contractors must protect; revise the in-force DOD regulations that require safeguards and govern breach reporting by defense contractors; and enhance the process and particulars of the safeguards contractors are to employ.

Industry supports the goal of these initiatives. But their accomplishment is difficult. Continuing exchanges between federal agencies and industry stakeholders are needed. The federal government should strive for consistency in requirements imposed upon its contractors. Improved cybersecurity is necessary to protect the confidentiality of sensitive but unclassified federal information. It is well established that economic espionage directed against the defense supply chain has resulted in serious harm to our military capabilities. It is urgent that the defense supply chain effectively improve defenses against these kinds of attacks. Lessons learned through implementation of the DOD cyber initiatives, affecting its contractors, should guide other federal agencies in the measures they will take to assure appropriate security for the many categories of CUI that are shared with non-federal partners.

This White Paper examines actions of the National Archives and Records Administration (NARA), the Department of Homeland Security (DHS), the Department of Defense (DOD) and the National Institute of Standards and Technology (NIST), a unit of the Department of Commerce. NARA holds the responsibility to identify and categorize all forms of CUI, for all agencies, where protection is required by law, regulations and governmentwide policies. Implementation of the NARA CUI Rule will involve actions by all federal departments and agencies to include, in agreements with non-federal entities, obligations to safeguard CUI in accordance with NIST SP 800-171. The White Paper endorses the efforts of NARA to achieve consistency and uniformity in the categorization, designation and protection of all types of CUI. Within the government, there should be consistency in the recognition and protection of CUI categories, rather than allowing any agency to create its own types of CUI. The federal government also should be consistent in the basic cyber safeguards that it applies for all CUI types. Industry would be frustrated if different agencies employ varying safeguards for information of a common CUI type.

The Paper recognizes the importance of the NARA effort and its difficulty. Several years will be required for implementation within federal departments and agencies. NARA is now working on a new Federal Acquisition Regulation (FAR) of general applicability for agencies to use to secure CUI by contract or other form of agreement. It will take time to develop and apply these new regulations and it is crucial that stakeholders (inside and outside of the government) have opportunity to participate in the rulemaking. At this stage, as NARA works to craft the general FAR, it is essential to adopt a prudent and achievable strategy that rests upon core principles of consistency and uniformity.

The Proposed DHS HSAR, examined in the light of these principles, suffers from a number of key deficiencies. Specifically, the HSAR would create several new categories of CUI that are not among those identified by NARA. One such category, "Homeland Security Agreement Information," is so broadly defined that it could allow DHS to designate any information exchanged via any agreement as this CUI type. Although the DHS rule ostensibly is to address CUI, it does not rely upon or even use the NIST SP 800-171 safeguards that the NARA Rule determined are to be used by all federal departments and agencies to protect CUI. (DOD uses SP 800-171 for its "Controlled Technical Information" of military and space significance and for all other forms of CUI.) The Proposed HSAR does not inform contractors and other non-federal partners of what security standards they will be required to use. In several aspects the rule seems to apply to non-federal entities who have DHS CUI the same rigorous, prescriptive and expensive requirements that are now required of federal agencies, and "Federal information systems." Such requirements have evolved for federal agencies to comply with the Federal Information System Modernization Act (FISMA). They should not be applied to non-federal entities simply because they are afforded access to CUI in the course of performing an agreement to supply a product or deliver a service.

DOD is the first federal agency to mandate cyber protection of CUI through contract requirements imposed on all DOD suppliers (except pure COTS products). Through the 'Network Penetration' DFARS, DOD requires contractors to have "adequate security" and to implement the 110 safeguards in SP 800-171 by no later than December 31, 2017. DOD's rules have been evolving since 2013. The most recent change, of October 21, 2016, includes some improvements but leaves several crucial areas unresolved. The defense industry supports DOD's objectives and shares the priority for improved information protection. But clarifications to the DFARS and changes to implementation and administration are necessary for industry to be successful in compliance and security improvement.

The White Paper looks carefully at five areas. The first is **designation**. DOD should accept that it is responsible to identify and designate the "Covered Defense Information" (CDI) that contractors are obliged to protect. It will greatly improve the ability of contractors to comply if DOD confirms that contactors only have to protect information that DOD has designated as CDI, and that such obligations are only "prospective" (newly received information) and not "retrospective" or inclusive of information received over prior years.

The second issue is **scope**. Here, the White Paper urges DOD to establish that it expects contractors to protect information that DOD has identified as CDI and provided to the contractor in the course of performance of a contract that is subject to the DFARS. The White Paper recommends revision to the DFARS definition of "Covered Defense Information" and removal of confusing language that can be interpreted to require protection of "background" business information and other data that a contractor may possess and use but which has only an attenuated or remote nexus to a DOD contract.

As to **methods**, the third issue, the focus is upon permissible use of cloud services. The recent revision to the DFARS now allows DOD contractors to use external cloud service providers (CSPs), where CDI is involved, only if those CSPs meet the security requirements of FedRAMP Moderate "or equivalent." This is insufficiently informative – what is meant by "or equivalent" and who decides – and too restrictive. DOD needs to spell out how it will determine what cloud security meets SP 800-171 and the DFARS. A security "overlay" should be prepared by NIST to describe what is needed, beyond the -171 controls, for CDI on an external cloud. It is not necessary to impose the whole of the FedRAMP process and federal-specific controls on external cloud providers; there are equally good, if not better, security methods that employ commercially accepted standards and practices.

With respect to the fourth issue, **adoption**, attention is directed to how DOD can improve the ability of small business to affordably and successfully implement the required security controls. DOD continues to depend on small business for many needs, and seeks the innovation of small business. The 'Network Penetration' DFARS are an obstacle and burden on smaller businesses, and yet security is just as important at the lower levels of the supply chain as at the top. Several specific recommendations are made as to how DOD can reach and assist the small business community. One recommendation is to make increased use of the NIST Cybersecurity Framework.

The fifth issue is **compliance**. DOD has taken a flexible approach to implementation and administration of the DFARS. But contractors are required to represent that they will deliver "adequate security" and fully implement the SP 800-171 controls by no later than December 31, 2017. DOD needs to better inform and assist its contractors so that they have confidence the security measures they adopt will satisfy DOD's requirements should they come under scrutiny following a cyber incident. The White Paper considers and recommends a number of different ways in which a "safe harbor" can be created and made accessible to contractors. A key component is contractor documentation of their security assessment and plans through the "System Security Plan" (SSP) that has been newly added as a requirement to SP 800-171. DOD has many options in how it can utilize the SSP, both for its own assurance purposes and to inform contractors they are on the right track.

The final section of the White Paper concerns Revision 1 to NIST SP 800-171. Although the changes were not numerous, they are important. Rev. 1 added, as a 110th security control, the obligation to prepare a System Security Plan. NIST is commended for this step, and for its

decision to let contractors make their own, business-appropriate decision as to the composition of the SSP. The SSP plays a key role, in documenting the contractor's assessment, identifying shortfalls and vulnerabilities, and describing the mitigation plan. The Paper also recognizes and credits NIST for its new efforts to prepare a compliance tool, NIST SP 800-171A, intended for Fall 2017 release, as a companion to SP 800-171.

Table of Contents

White Paper

Federal Actions to Enable Contractors to Protect "Covered Defense Information" and "Controlled Unclassified Information"

By Robert S. Metzger[i]

Over the past six months, important actions have been taken by the federal government to safeguard the confidentiality of information that the government provides to or receives from its suppliers. On September 14, 2016, the National Archives and Records Administration (NARA) published the final rule, "Controlled Unclassified Information" (CUI).[2] The Department of Defense (DOD), on October 21, 2016, revised and finalized the Defense Federal Acquisition Regulation Supplement (DFARS) rule, "Network Penetration Reporting and Contracting For Cloud Services."[3] The National Institute of Standards and Technology (NIST), on December 21, 2016, issued Revision 1 to Special Publication (SP) 800–171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." These actions (i) establish the process by which agencies designate federal information which contractors must protect; (ii) revise the DOD regulations that require safeguards and govern breach reporting by defense contractors; and (iii) enhance the process and particulars of the safeguards contractors are to employ.

Industry supports the goal of these initiatives. But their accomplishment is difficult. Continuing exchanges between federal agencies and industry stakeholders are needed. The federal government should strive for consistency in the requirements it imposes upon its contractors – whether for DOD or civilian agencies.

The impact of cyber threats to the defense supply chain is widely recognized. Cyber-attacks upon the supply chain have resulted in the unauthorized exfiltration – "theft" – of valuable and sensitive defense information.[4] Senior defense officials have expressed alarm at the persistent and pervasive economic espionage that has been accomplished by adversary exploits of cyber vulnerabilities among federal suppliers. The national interest has been harmed. Rivals and adversaries are able to mimic U.S. capabilities without making their own investment. They seek to deny or degrade the advantage that the U.S. sought to obtain through our advanced technologies. Analysis of past attacks indicates that adversaries often direct their attacks at links in the supply chain, such as smaller companies or commercial concerns, where cyber defenses may be weakest. Key defense information resides not only on the Pentagon's own information systems, or those operated by contractors on behalf of DOD: it resides also at all levels of the supply chain, from the large prime contractors to small businesses who perform key, specialty functions.

---

[2] 81 Fed. Reg. 63324 (Sep. 14, 2016).
[3] 81 Fed. Reg. 72986 (Oct. 21, 2016).
[4] DOD recently revised Department of Defense Instruction (DODI) 5000.02 adding new emphasis to cybersecurity in the defense acquisition system. Cyber impact on defense acquisitions includes, as examples of malicious activity, exfiltration of operational and classified data, exfiltration of intellectual property and designs, insertion of compromised hardware, and subversion of networks. DODI 5000.02, Change 2, Feb. 2, 2017, Enclosure 14, at 171, at http://www.dtic.mil/whs/directives/corres/pdf/500002_dodi_2015.pdf.

Since 2013, DOD has used acquisition regulations to protect "Controlled Technical Information" (CTI) of military or space significance.[5] Other forms of information may not have military or space significance, but loss of confidentiality through a cyber breach, can produce serious, even grave national injury. The eventual consequences of the 2015 attack upon federal personnel records are not yet known, but it is self-evident that serious risks to national security are present in that the security clearance records of 21.5 million persons were compromised by exfiltration.[6] Hostile exploitation of stolen information about individuals could frustrate law enforcement and enable subversion of many government activities, such as identity validation for international travel, eligibility for government benefits, filing of false tax returns, and fraudulent receipt of healthcare benefits, among others.[7]

Federal agencies are obligated by statute to protect federal information and federal information systems. The same information is made accessible to hundreds of thousands of non-federal entities – contractors, grantees, state and local governments, educational institutions, and others – pursuant to contract or other form of agreement. All of this information is at risk, whether on a federal or non-federal information system, and the impact of successful extraction, unauthorized exploitation or corruption depends upon the nature of the information rather than the locale of or authority over the information system that was breached. These conditions explain the great importance of the federal campaign to improve the cyber protection of all forms of controlled unclassified information, whether inside or outside the federal government.

This White Paper examines recent developments and considers principal sources of confusion and complaint, whether the federal initiatives are working, and how to improve regulation and practice so that more companies and other non-federal entities can affordably and promptly achieve adequate security and comply with new requirements.

I. THE FINAL CUI RULE

NARA has been assigned by Executive Order the responsibility to coordinate among all federal agencies to establish rules for designation, dissemination and protection of all forms of CUI.[8] Driving the initiative has been the requirements of FISMA - the Federal Information Security Modernization Act of 2015, Pub. L. 113–283, 44 U.S.C. § 3554. The CUI Final Rule establishes a policy that "[a]ll unclassified information throughout the executive branch that requires any safeguarding or dissemination control is CUI."[9]

---

[5] *See* DFARS, "Safeguarding Unclassified Controlled Technical Information," Final Rule, 78 Fed. Reg. 69273 (Nov. 18, 2013). The formal definition of "CTI" may be found in the CUI Registry, available at https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html;
[6] This kind of "identity theft" has public consequences well beyond any remediation as individuals might receive through after-the-fact identity protection and credit monitoring. Malicious actors now use stolen Personally Identifiable Information ("PII"), in conjunction with modern technology and forged identity documents, for social engineering purposes that include "synthetic identity theft, which occurs when a malicious actor constructs a new identity using a composite of multiple individuals' legitimate information along with fabricated information." Office of Management and Budget ("OMB"), "Preparing for and Responding to a Breach of Personally Identifiable Information," Memorandum M-17-12, Jan. 3, 2017, at 6.
[7] Id.
[8] Executive Order 13556, "Controlled Unclassified Information," Nov. 4, 2010, at Sec. 2(c).
[9] Controlled Unclassified Information Final Rule ("CUI Final Rule"), § 2002.1(c), 81 Fed. Reg. 63225 (Sep. 14, 2016).

A. NARA's Intended Operation of the CUI Rule

The CUI Final Rule obligates agencies to safeguard all CUI. The "CUI Registry," maintained by NARA, includes authorized CUI categories and subcategories.[10] It presently identifies 23 categories and 84 subcategories of CUI. The CUI Final Rule reaches beyond federal agencies to extend to any non-federal entity that may be afforded access to any form of CUI:

> "When the Government provides controlled information to a non-executive branch entity, sometimes pursuant to a contract or other agreement, it does not make sense for the protection requirements to disappear or lessen just because the Government has shared the information. In fact, the protection requirements do *not* disappear or lessen."[11]

What are "non-executive branch" entities? In comments accompanying promulgation of the CUI Final Rule, NARA explains:

> "(gg) Non-executive branch entity is a person or organization established, operated, and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include: Elements of the legislative or judicial branches of the Federal Government; state, interstate, tribal, or local government elements; and private organizations."[12]

NARA has estimated there are 300,000 such entities which receive, host or use one or another form of CUI.[13] Even if the actual number is only a fraction of this figure, the CUI Rule has great potential impact upon many and diverse non-federal entities, few of whom may now anticipate they will become subject to CUI protection obligations.

A crucial distinction in the CUI rule is between "Federal information systems" and "non-Federal information systems."[14] The former is "an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." As to federal information on these systems, the CUI rule requires agencies to apply security requirements and controls from Federal Information Processing Standard (FIPS) Publication 200 and NIST Special Publication (SP) 800-53.[15] The CUI rule also sets the baseline for "confidentiality impact level" for CUI, under FIPS 199, at "Moderate". Notably, the CUI rule also states:

---

[10] Id. at § 2002.10, 2002.12(a).
[11] The CUI Registry is available at https://www.archives.gov/cui/registry/category-list. "Controlled Technical Information" is one of the 23 categories.
[12] CUI Final Rule, 32 CFR at § 2002.4(gg).
[13] Adam Mazmanian, "NARA Preps for New Info Control Rules," *Federal Computer Week*, May 28, 2015 (statement attributed to John P. Fitzpatrick, former director of the Information Security Oversight Office).
[14] CUI Final Rule, at § 2002(h).
[15] Id. at § 2002(g).

> "Agencies may increase CUI Basic's confidentiality impact level above moderate only internally, or by means of agreements with agencies or non- executive branch entities (including agreements for the operation of an information system on behalf of the agencies). Agencies may not otherwise require controls for CUI Basic at a level higher or different from those permitted in the CUI Basic requirements when disseminating the CUI Basic outside the agency."[16]

This provision reflects the objective of NARA, consistent with the Executive Order, to achieve consistency and uniformity in federal application. Agencies are not to act unilaterally to create their own categories of CUI or to impose higher levels of controls upon contractors or other non-federal CUI recipients.

In parallel, the CUI rule specifically limits what controls may be imposed by agencies upon non-federal information systems, i.e., those operated by contractors not "on behalf of" an agency but for their own business purposes. The CUI rule states unequivocally that agencies "may not treat non-Federal information systems as though they are agency systems" and that NIST SP 800-171 defines the requirements to protect CUI basic on non-federal information systems.[17] There is no latitude for variance at the preference of an agency:

> "Agencies *must use NIST SP 800–171* when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless 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)."[18]

Thus, the CUI Final Rule incorporates by reference NIST SP 800-171 and obligates its use when agencies establish security requirements to protect CUI's confidentiality on non-federal information systems.[19] Industry has many reasons to support NARA's approach. There is clear demarcation, in the CUI rule (and in NIST publications), between the cybersecurity requirements imposed on contractors who operate a "Federal information system," on the one hand, and those who may receive CUI and host or process it with a contractor (non-federal) information system. The obligations for cyber protection differ greatly between the categories – SP 800-53 versus 800-171. It will only confuse industry and frustrate achievement of security if federal agencies and departments decide, on their own, and without basis in law, regulation or Government-wide policy, to subject private companies to the much more onerous requirements applicable to federal agencies.

---

[16] Id.
[17] Id. at § 2002(h)(2).
[18] Id. (emphasis added)
[19] Id. at § 2002.15(h)(2).

The Department of Homeland Security, however, has issued a Proposed Rule that would do just that. It would add new categories of CUI that are not reflected in the CUI Registry. It would blur if not eliminate the distinction between federal information systems and non-federal systems, such that many companies could be swept unknowingly into requirements that far exceed those of SP 800-171. This Proposed Rule is discussed further, below.

The CUI Final Rule contemplates that all agencies will enter into "agreements" with any "non-executive branch" entity to share CUI.[20] The Rule, including SP 800-171 safeguards, is to be applied "through incorporation into agreements."[21] NARA expects that all federal agencies will come to utilize contract or agreement provisions to impose mandatory safeguards on non-executive branch entities for all forms of CUI:

> "The [CUI] rule now says that it applies only to executive branch agencies, but that, in written agreements (including contracts, grants, licenses, certificates, and other agreements) that involve CUI, agencies must include provisions that require the non-executive branch entity to handle the CUI in accordance with this rule, the Order, and the CUI Registry."[22]

Today, there is no established federal regulation by which civilian agencies apply CUI protection requirements to non-executive branch entities. Nor have the civilian agencies fully implemented the rule. In fact, federal agencies are to establish a "management and planning framework" for "phased implementation."[23] It will take several years for agencies to fully implement the CUI Final Rule, because it affects many areas of agency operation, including determination of which information qualifies as what type of CUI, how to affix CUI designations or "legends" upon both physical and electronically stored information, physical protection controls, dissemination limitations, compliance with the Privacy Act of 1974, and public access – among many subjects.

Until civilian agencies have made further progress with implementation of the rule, enforcement of mandated cyber safeguards upon non-federal entities will be problematic, if for no other reason than that agencies did not identify or designate as CUI information previously made accessible to contractors and other entities. This is a key point. Where DOD, DHS or any federal agency requires its contractors or non-federal partners to protect CUI, it is the responsibility of the agency to **identify** and **designate** the information that is to be protected. The Department of Defense, at present, is the only federal agency that requires its contractors to safeguard all forms of CUI as contemplated by NARA's CUI Final Rule. It does so through solicitation requirement and contract terms, promulgated through the DFARS, as further discussed below.

---

[20] Id. at §§ 2002.4(c), 2002.16(a)(6).
[21] Id. at § 2002.1.
[22] Id. at 63326. The CUI Final Rule states that "[a]gencies should enter into agreements with any nonexecutive branch or foreign entity with which the agency shares or intends to share CUI." Id. at § 2002.16 (a)(5)(i). The Rule also states that such agreements, "[a]t a minimum," must include provisions that obligate non-executive branch entities to handle CUI in accordance with the Rule and NARA's CUI Registry. Id. at § 2002.16(a)(6).
[23] Id. at § 2002.8(a)(6)

B. The Proposed DHS Rule

The Department of Homeland Security, however, recently published a proposed rule, "Homeland Security Acquisition Regulation (HSAR); Safeguarding of Controlled Unclassified Information."[24]

1. Addition of "New" Categories of DHS CUI

In apparent conflict with the express language of the Final CUI Rule, the proposed DHS Rule would add four new categories of DHS CUI not among those now recognized by NARA. The four new categories or subcategories of CUI are Homeland Security Agreement Information, Homeland Security Enforcement Information, Operations Security Information, and Personnel Security Information.[25] On its face, the addition of four categories of CUI, at the initiative of this one agency, seems contrary to the CUI Final Rule. In that Rule, NARA stated that "the CUI Registry lists categories and subcategories of CUI that laws, regulations, and Government-wide policies create or govern".[26] The Final CUI Rule states:

> "Agencies may use *only* those categories or *subcategories approved by* the *CUI EA* [Executive Agent - NARA] and published in the CUI Registry to designate information as CUI."[27]

Moreover, the Final CUI Rule explicitly "overrides agency-specific or *ad hoc* requirements when they conflict."[28] As NARA explained in the preface to the Final CUI Rule, the structure of the rule, the CUI Registry, NIST standards, and oversight functions of NARA as the CUI Executive Agent "are designed to restrain over-broad application."[29]

One of the new categories, "Homeland Security Agreement Information," is especially problematic. As defined in the proposed HSAR:

> "(4) Homeland Security Agreement Information means information DHS receives pursuant to an agreement with state, local, tribal, territorial, and private sector partners that is required to be protected by that agreement. DHS receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Security Act."[30]

Essentially, this allows DHS to determine, agreement-by-agreement, what information exchanged under that agreement is to be protected by the rule. The CUI Rule seeks to establish consistency

[24] 82 Fed. Reg. 6429 (Jan. 19, 2017).
[25] Proposed HSAR 3052.204-7X(a)("Definitions").
[26] 81 Fed. Reg. 63325, 63326 (Sep. 14, 2016).
[27] CUI Final Rule, at § 2002.12(b) (emphasis added).
[28] Id. at § 2002.1(i).
[29] 81 Fed. Reg. 63328 (Sep. 14, 2016).
[30] Proposed HSAR, at § 3002.101 (Definitions), at 82 Fed. Reg. 6441 (Jan. 19, 2017).

and predictability – for the benefit of both federal agencies and departments as well as non-federal entities that may receive or generate CUI. For this reason, the definition of CUI is –

> "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."[31]

There is an obvious tension between the plain words of the Final CUI Rule (as emphasized above) and the category of "Homeland Security Agreement Information" proposed by DHS, because DHS proposes that it can decide, on an individual contract, what information is to be protected "in furtherance of the missions of the Department." This is not protection of an "information type" and there is no constraint that DHS limit designation to information where safeguards are required by law, regulation, or Government-wide policy. To the contrary, DHS would reserve unto itself, by contract, to designate data. Crediting DHS with good intentions, DHS non-federal partners should be troubled by this proposed new, DHS-unique, contract-specific form of CUI. It will be extremely difficult to plan for or administer information system protections if the agency can decide, for and during performance of a contract, that some information must be protected even if it does not "fit" within one of the established CUI Categories and Subcategories.

2. Safeguards for DHS CUI Differ from SP 800-171

The proposed HSAR requires safeguarding of CUI for two very different categories of contractor activity. The first is where DHS CUI is on a contractor information system that the contractor operates on behalf of DHS. The second is where DHS CUI resides on the contractor's information system which it uses to perform a DHS agreement.

- Contractors Who Use DHS CUI to Operate a Federal Information System for DHS. In the first category, as the proposed rule recognizes, the contractor is operating a "Federal information system" by or on behalf of the agency. The proposed rule applies to a contractor in this category the full range of federal obligations that apply to agencies.[32]

- Other Contractors Who Have Access to DHS CUI. The second category applies to the non-federal entities allowed access to DHS CUI by the agency. These contractors and subcontractors – who are *not* operating a "Federal information system" – "must provide adequate security to protect CUI from unauthorized access and disclosure."[33]

[31] CUI Final Rule, at § 2002.4(f) (emphasis added).
[32] Proposed HSAR, at § 3052.204-7X(c). A contractor in this category "shall not collect, possess, store or transmit CUI" without an Authority to Operate (ATO) that has been accepted by DHS. An extensive and rigorous process is described, including a Security Authorization process, requirements to develop a Security Authorization Package, independent assessment, periodic ATO renewal, mandatory consent to random periodic security reviews, compliance with federal reporting, obligatory continuous monitoring, incident reporting and response – and more.
[33] Id. at § 3052.204-7X(b).

At first blush, these provisions seem aligned with the Final CUI Rule. But they are not, upon further examination.

Had it followed the Final CUI Rule, DHS would have caused its agreements with non-federal entities to include requirements to safeguard DHS (or other CUI) in accordance with SP 800-171. This approach was not chosen.

Contractors and subcontractors must provide "adequate security" to protect CUI, which is defined as "compliance with DHS policies and procedures in effect at the time of contract award."[34] It does not utilize SP 800-171; instead, the proposed HSAR refers to "policies and procedures" said to be "accessible at http://www.dhs.gov/dhs-security-and-trainingrequirements-contractors." That link, however, points to two DHS directives that pre-date the NARA CUI Final Rule; no mention of any NIST standard is contained in either.

In fact, the proposed HSAR does not inform non-federal entities what "**safeguards**" are to be applied. Nor does it discuss who has the responsibility to identify or designate DHS CUI, whether any safeguarding obligations also apply to other categories or subcategories of CUI as listed in the Federal Registry, what relationship must exist between the presence of information that could be CUI and a contractual obligation to DHS, or how the agency will respond, advise or adjudicate any questions as to application, administration, implementation or enforcement of the safeguarding obligation. This leaves a vast area of uncertainty.

There is no room for doubt that DHS intends to obligate any contractor (or subcontractor) to safeguard DHS CUI, even when it is on a contractor information system that is not a "Federal information system":

> "DHS requires that CUI be safeguarded wherever such information resides. This includes government-owned and operated information systems, government-owned and contractor operated information systems, contractor-owned and/or operated information systems operating on behalf of the agency, and any situation where contractor and/or subcontractor employees may have access to CUI. There are several Department policies and procedures (accessible at http://www.dhs.gov/dhs-security-andtraining-requirements-contractors) which also address the safeguarding of CUI. Compliance with these policies and procedures, as amended, is required."[35]

In this language, DHS conflates the two fundamentally different categories of information system – those which are operated by or "on behalf of an agency" (a "Federal information system") and those which are operated by a contractor for its own purposes incidental to the delivery of supply or service to a federal customer (a non-federal information system). As explained above, the Final CUI Rule was clear that federal agencies are *not* to impose the requirements of the

[34] Id. at § 3052.204-7X(c).
[35] Proposed HSAR Section 3004.470-3(a) (Policy).

former on the latter.[36] DHS has not explained the basis for its deviation from the Final CUI Rule. It is not sound policy. It would enable one agency to impose different (and presently unknown cyber safeguards) than do other agencies for information that is also CUI and also has "Moderate" impact. It would leave contractors to guess what security controls may apply. To the extent DHS intends to pull its contractors towards SP 800-53, DHS would obligate those companies to employ federal-specific control methods to the same kind of information that, under SP 800-171, could be protected by means more accommodating of existing contractor methods and commercial best practices.[37]

The *only* mention to SP 800-171 in the proposed HSAR to safeguard CUI is in a footnote in the preamble to the rule.[38] Although DHS allows that it is "aware" of SP 800-171, and that it was released to provide federal agencies with recommended requirements for CUI, DHS insists that "the information system security requirements in this proposed rulemaking are focused on Federal information systems, which include contractor information systems operating on behalf of an agency", and such systems "are not subject" to SP 800-171.

While the drafters may have "focused" on DHS contractors who operate a Federal information system, the Proposed HSAR is **not** limited to just to them. For illustration, the following statement is contained in the required analysis under the Regulatory Flexibility Act:

> "This rule *will apply to DHS contractors that require access to CUI*, collect or maintain CUI on behalf of the Government, **or** operate Federal information systems, which includes contractor information systems operating on behalf of the agency, that collect, process, store or transmit CUI."[39]

As presently drafted, the term "or" would be interpreted in the **conjunctive**, meaning that the rule applies to DHS contractors that "require access to CUI" and, distinctly, to DHS contractors who collect or maintain CUI, or to those who operate a "Federal information system". Another statement is that "adequate security" requirements apply "when contractor and/or subcontractor employees will have access to sensitive CUI."[40] In the same analysis, DHS refers to its award, for FY 2014, of nearly 14,000 new contracts to large and small businesses. By no means were **all** of these contracts for operation of a "Federal information system". DHS says that "a number of factors determine applicability of the proposed clause".[41] The proposed "Safeguarding" clause

---

[36] As explained by NARA in the comments that preceded the Final CUI Rule: "The NIST SP 800–171, incorporated by reference in this final rule, establishes guidance for protecting CUI in non-federal systems: (1) When the CUI is resident in non-federal information systems and organizations; (2) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and (3) when the authorizing law, Federal regulation, or Governmentwide policy listed in the CUI Registry for the CUI category or subcategory does not prescribe specific safeguarding requirements for protecting the CUI's confidentiality." 81 Fed. Reg. 63325 (Sep. 14, 2016).
[37] SP 800-171 describes 110 controls in 14 families of security requirements. The families and controls in SP 800-171 align to corresponding principles in FISMA, which applies to federal agencies and federal information systems. SP 800-171 articulates safeguards as *objectives* but deliberately does not require contractors to follow the specific controls and enhancements elaborated in SP 800-53, which NIST developed for federal information systems that are subject to FISMA information security requirements.
[38] 82 Fed. Reg. 6431, n.5 (Jan. 19, 2017).
[39] 82 Fed. Reg. 6439 (Jan 19, 2017) (emphasis added).
[40] Id.
[41] Id.

says that "[c]ontractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure."[42] This obligation is not confined only to contractors operating a Federal information system. The "adequate security" obligation appears to apply to every DHS contractor (and every subcontractor, at any level) who is allowed access to DHS CUI.

The neglect of SP 800-171, despite recognition of its intended purpose, is neither explained nor justified. If the HSAR were to take effect as presently drafted, at best it would leave thousands of contractors and subcontractors completely "in the dark" as to what safeguards would satisfy their obligations to DHS.[43] Reference to security requirements that are "to be determined" in the future does not inform contractors how to plan or implement. The proposed HSAR is both incomplete, by its terms, and inconsistent with the Final CUI Rule. As shown below, it is also inconsistent with the approach that DOD has taken in the 'Network Penetration' DFARS, which applies to NARA CUI Categories and relies upon security controls from NIST SP 800-171. DOD has publicly endorsed NIST SP 800-171 as allowing non-federal organizations to consistently implement safeguards for the protection of CUI – "one CUI solution for all customers" – but the proposed DHS HSAR would produce an opposite, and undesirable result.

3. Other Questionable Features

Fundamentally, the Proposed HSAR may follow from a mindset that DHS has key information to protect and is prepared to do business only with contractors who will invest and secure their on-premises information systems and monitor these systems as DHS specially requires. That will narrow DHS' access to sources. It likely will add to acquisition costs. Surprisingly, the proposed HSAR does not recognize or accommodate the use of cloud services by its contractors in either category of access to DHS CUI.[44]

The rule also describes itself as having "requirements ...expanded to include professional services contractors that have access to CUI."[45] Because it does not clearly articulate how requirements would be applied to professional service providers, what safeguards they would be obligated to provide, or how they would be assessed by DHS, the professional services community will be uncertain how to prepare or comply.

Small businesses also should be concerned. DHS acknowledges that this is a "significant" regulatory action and that will have impact on small business.[46] DHS seems resigned to high

[42] Proposed HSAR 3052.204-7X(b)(1).
[43] The proposed rule says that the Government will provide a "Requirements Traceability to Matrix (RTM)" (sic) so that "contractors will know *at the solicitation level* the security requirements for which they must comply." 82 Fed. Reg. 6437 (Jan. 19, 2017) (emphasis added). The RTM is directly linked to the requirements for a contractor's security authorization package - itself an obligation imposed only on those "first category" contractors who operate a federal information system for DHS. The intent of DHS to prepare a RTM for individual solicitations suggests that there could be many variations of security requirements, such that an authorization package for one DHS requirement may not suffice for others. While this can be the necessary and prudent approach where a non-federal entity is operating an information system "on behalf of DHS," it will cause great frustration to non-federal entities that have access to DHS on their enterprise systems.
[44] The only reference to "cloud" is that DHS received input from FedRAMP for the costs of independent assessment of security methods. 82 Fed. Reg. 6434 (Jan. 19, 2017).
[45] 82 Fed. Reg. 6439 (Jan. 19, 2017).
[46] 82 Fed. Reg. 6443, 6439 (Jan. 19, 2017).

costs of consultants and systems. DHS "invites comments from small business concerns … on the expected impact of this rule on small entities," but there is nothing specific to assure the small business community that it will be able to comply.

C. The Anticipated "General FAR CUI Rule"

NARA's intent was to lead development of a "General FAR CUI Rule" that – when finalized – will obligate all federal agencies to require cyber protection of CUI, per SP 800-171, in all contracts and agreements.[47] As of March 6, 2017, no formal FAR case to implement the CUI rule is open and reported publicly.[48] Whether the FAR case has been delayed, and why, are not known. The rulemaking could be affected by the reported regulatory "freeze" implemented by the new Administration. Delay creates its own problems. The NARA CUI rule is final, and therefore operates upon all federal agencies. Part of the rule is the extension of the SP 800-171 safeguards to non-federal entities who access CUI. That is accomplished through contract or agreement terms which, in turn, are to be established through regulation. Without completion of the General FAR CUI Rule, there will be no prevailing way for agencies to obligate non-federal recipients to protect CUI. This will encourage some agencies – as evident from the recent proposed DHS HSAR – to go their own way. As agencies act independently to obligate their non-federal partners to protect agency-specific CUI using agency-distinct safeguards, the prospect looms of inconsistent if not chaotic demands upon contractors and other non-federal entities – all to achieve the common purpose of safeguarding CUI.

NARA has assumed a very difficult task in seeking "one rule" to bind all the agencies as to classification, designation, dissemination and safeguarding of CUI. But there are powerful benefits to this integrated approach. It reduces diversity among federal agencies and promotes common practices and consistent security methods. (These objectives may be consistent with higher level cybersecurity goals of the new Administration.) At the same time, care is needed in the formulation of regulations and contract requirements. The General FAR CUI Rule could apply to as many *several hundred thousand* non-federal entities, according to prior NARA estimates. This is a much larger universe than the approximately 10,000 contractors who are subject to the DFARS cyber rules. Despite years of gestation to reach the current rule, many problems remain in the implementation of DFARS requirements. The experience of government and industry with the DFARS should guide the development and application of the General FAR CUI rule.

Industry and government should collaborate to address a key question – namely, how can government be assured of contractor compliance with the security requirements without imposition of a costly, intrusive regime of government oversight, assessment or authorization? As discussed below, SP 800-171 now requires preparation of a system security plan – a self-assessment and plan of action to mitigate identified gaps. Federal agencies may need to develop capable resources to review such plans when a contractor chooses to submit them for

[47] As explained by NARA, "the CUI EA [Executive Agent] is developing a Federal Acquisition Regulation (FAR) case through the normal FAR process, for agencies to use in contracts". 81 Fed. Reg. 63324, 63328 (Sep. 14, 2016).
[48] *See* "Open FAR Cases as of 3/6/2017," available at http://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf.

federal assessment – or is required to do so. The General FAR CUI Rule should inform industry of the systems, policies and practices sufficient to earn "safe harbor" from contractual or other liability for a cyber breach, should one occur that affects CUI.

II. THE REVISED NETWORK PENETRATION DFARS

DOD's efforts to protect information of military or space significance have a comparatively long history. On November 18, 2013, DOD issued a Final Rule, "Safeguarding Unclassified Controlled Technical Information," that applied some cyber safeguards derived from NIST SP 800–53 to "Controlled Technical Information."[49] During 2015, DOD twice revised the rule.[50] As revised on Dec. 30, 2015, companies were obligated to protect "Covered Defense Information" (CDI). CDI was defined to include four categories of information – Controlled Technical Information, Critical Information (Operations Security), Export-Controlled Information, and a "catch-all" category, namely any other information that requires safeguarding pursuant to "law, regulations and Governmentwide policies".[51] For safeguards, NIST SP 800-171 displaced controls drawn from SP 800-53 as had been invoked by the earlier UCTI Rule.[52] By the Dec. 30, 2015 Interim Rule, Contractors were required to report on any gaps against NIST SP 800-171 safeguards within 30 days of receipt of a contact subject to the DFARS clause but were not held to be in full compliance with SP 800-171 until December 31, 2017.[53]

Significant changes were made on October 21, 2016, with the DFARS Final Rule.[54] The most important were the: (i) revised definition of "Covered Defense Information"; (ii) exclusion of COTS acquisitions; (iii) expanded authorization for use of cloud services; (iv) exclusion of fundamental research; (v) additional guidance on how to vary from SP 800-171 requirements or seek approval of the DOD CIO; (vi) authorization to higher tier contractors to flow down the –7012 clause only when CDI is necessary for performance of the subcontract; and (vi) provisions that "any individual, isolated, or temporary deficiencies" may be addressed in a system security plan (SSP).[55] In addition, at the same time as DOD issued the revised Final Rule, it made available

[49] Final Rule, "Safeguarding Unclassified Controlled Technical Information," 78 Fed. Reg. 69273 (Nov. 18, 2013).
[50] Interim Rule, "Network Penetration Reporting and Contracting for Cloud Services," 80 Fed. Reg. 51739 (Aug. 26, 2015); and Interim Rule, "Network Penetration Reporting and Contracting for Cloud Services," 80 Fed. Reg. 81472 (Dec. 30, 2015).
[51] DFARS 252.204-7012 ("Safeguarding Covered Defense Information and Cyber Incident Reporting") (AUG 2015) (definition of "Covered Defense Information").
[52] In explaining this change, DOD stated: "NIST SP 800–171 is a publication specifically tailored for use in protecting sensitive information residing in contractor information systems that refines the requirements from Federal Information Processing Standard (FIPS) 200 and controls from NIST SP 800–53 and presents them in an easier to use format. In addition to being easier to use, NIST SP 800–171 greatly increases the protections of Government information in contractor information systems, while simultaneously reducing the burden placed on the contractor by eliminating Federal-centric processes and requirements currently embedded in NIST SP 800–53." 80 Fed. Reg. 51740 (Aug. 26, 2015).
[53] DFARS 252.204-7008 ("Compliance with Safeguarding Covered Defense Information Controls.") (DEC 2015) (c)(1); *see* 80 Fed. Reg. 81473 (Dec. 30, 2015).
[54] 81 Fed. Reg. 72986 (Oct. 21, 2016).
[55] *See* 81 Fed. Reg. 72986, DFARS 252.204-7012(b)(3) (system security plan).

"Frequently Asked Questions" (FAQs) which address many issues of application or interpretation not covered by the regulations themselves.[56]

Many of these changes are helpful, but not all. Some key areas of application, adoption and compliance are not addressed sufficiently. These are, respectively, a **designation** issue of whether contractors are responsible to identify and mark CDI, even if the DOD customer has not; a **scope** issue of whether "CDI" includes information that did not originate with and is not delivered to the Government; a **methods** issue as to how contractors can utilize cloud services and comply; an **adoption** issue of how to assist small businesses to comply without driving them away from the defense supply chain; and the **compliance** question of what measures or processes are sufficient to assure companies that they fulfill the DFARS, satisfy SP 800-171 and will find "safe harbor" should an investigation follow a cyber breach.

A. Designation: Who Determines What is "Covered Defense Information"?

There are several parts to the definition of CDI. CDI now includes unclassified controlled technical information (CTI), with military or space significance, "or other information as described in the NARA CUI Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies", *and* the information must be either:

> "(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."[57]

The second part of the definition (items (1) and (2) above) deserves emphasis. Information is not subject to the DFARS unless it first qualifies as one of the established forms of CUI, including CTI, but then *only if* there is a sufficient nexus to the Federal government. The "easy" case is presented where the Government (DOD) identifies and designates information as CUI; as for CTI, for example, the information would bear one of the restricted "distribution statements" B through F in DODI 5230.24. Problems are presented, however, where DOD has not identified, or designated information as CDI, even if it is provided to a contractor in support of contract performance. More issues arise under the last "prong" of the definition – at what point is the

[56] The FAQs are periodically updated as DOD addresses additional implementation issues. As of this writing, there are 59 FAQs regarding the implementation of DFARS Subpart 204.73. "Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018) Frequently Asked Questions (FAQs)", Jan. 27, 2017, at http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf. The FAQs reflect DOD's exchanges with industry about DFARS implementation and contain much helpful guidance. However, many companies subject to the DFARS are unaware of the FAQs. Also, the FAQs have been criticized in some quarters as adding to the DFARS what it does not contain, varying from the DFARS, and for internal inconsistencies. Even so, DOD is to be commended for working to inform both DOD components and the contractor community, through the FAQs, on implementation issues and resolution.

[57] DFARS 252.204-7012(a) (Definitions).

relationship between a type of information, and federal ownership, authorship or control, so attenuated that it cannot be said to "support … the performance of the contract"?

Some controversy has attached to DOD's decision, in the Oct. 21, 2016 DFARS revision, to include all forms of CUI in the definition of the CDI that contractors must safeguard.[58] DOD's rationale is that all types of CUI, by definition, require protection by operation consistent with law, regulations and governmentwide policy. CTI is one of the 23 categories of CUI in the Registry, and every category (and all of the 82 sub-categories) merits protection. This is a reasonable proposition, in the abstract, and one that reflects current concerns about the damage to federal (versus individual) interests that can be accomplished through loss of confidential information such as PII or Protected Health Information (PHI). There are significant implementation problems, however.

The principal problem is that companies read the DFARS as requiring them to identify and protect all forms of CUI even though (a) the information may have been provided by or to civilian agencies before receipt of a DOD contract subject to the 'Network Penetration' DFARS; (b) such information may exist in electronic form without CUI designation originated by the responsible agency; and (c) companies have no ready method to differentiate the CUI that DOD expects them to protect from CUI that may have been obtained or created without any relationship to a DOD contract (or subcontract).

Uncertainty, as to the breadth of obligations to find and protect CUI, poses an obstacle to implementation and compliance. No federal civilian agency has fully implemented the Final CUI Rule and so there is an enormous volume of information that may fit a CUI category that has been shared with non-federal entities without CUI designation. It is practically impossible for DOD – or any other federal agency – to require contractors to "look back" and identify for protection CUI they may already have but which was not designated or identified when received.

As an urgent matter, DOD should revise the DFARS to clarify that the DFARS requires defense suppliers to only protect CUI that DOD furnishes to a contractor (or orders from it) in the performance of a contract subject to the -7012 "Safeguarding" clause, where DOD has identified and designated the information as CTI or any other CUI category.

Relatedly, DOD should clarify the DFARS, or otherwise inform contractors, that protection requirements are not applied retroactively; only CDI furnished by (or supplied to) DOD in the performance of a contract subject to the -7012 "Safeguarding" clause is subject to the requirements of "adequate security" and NIST SP 800-171.

[58] Also subject to protection and reporting requirements is "operationally critical support information," which concerns "supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation." Id. DFARS 252.204-7012 does not clearly include "operationally critical support" information in the definition of CDI and it is not among the categories or subcategories in the NARA CUI Registry. The DFARS states, however, that the -7012 clause must flow down to subcontracts that are for "operationally critical support," DFARS 252.204-7012(m)(1). In the FAQs, at Q&A 4, DOD asserts the requirements of 252.204-7012 "must be implemented when performance of the contract involves operationally critical support."

These measures would improve assurance of compliance and relieve companies of the potentially insoluble problem of having to look across whole enterprises to find information that "might" be CUI and to cause that information (physically or logically) to meet DFARS and SP 800-171 requirements. Initially, only DOD should identify and designate information as "CUI" because only DOD has implemented agency policy and acquisition regulations governing all categories of CUI. As and when civilian agencies identify and designate CUI, and adopt contract or agreement terms requiring its protection, at that time DOD contractors should protect such information when its source (or "destination") is other than DOD.[59]

Over time, contractors accumulate enormous quantities of information in electronic form. Some of that information could "fit" definitions of CUI as now are established. However, rarely did historically acquired information come with designation or marking as to its CUI status. It is not workable for the DFARS to require companies to protect "legacy" information, accumulated before receipt of a contract subject to the 'Network Penetration' DFARS. Moreover, there must be a "nexus" between a federal contract that is subject to the DFARS and the *subsequent* receipt or creation of information that DOD determines should be protected. Accordingly, DOD should explain that the DFARS imposes *prospective* obligations to identify and safeguard the CTI and other CUI that DOD identifies and designates.

Alternatively, DOD can decide to give priority to the protection of CTI – that of military or space significance. Many of the "other" CUI categories that concern *individuals*, such as PII and PHI, for example, are subject to separate laws or regulations that require protection. Consider DFARS implementation and the application of cyber safeguards as a business problem. An efficient solution to a business problem is one that is affordable (financially) and achievable (technically). From this standpoint, DOD could be justified to hold its suppliers to an earlier compliance date for CTI than for other forms of CUI if sequencing the obligation were to mitigate the burden on its suppliers, clarify what information constitutes a form of CUI that must be protected, and produce better security sooner for CTI.[60]

B. Scope: Does CDI Include "Non-Federal" Information?

Conceptually, the origin of the Network Penetration DFARS, and the purpose of the CUI initiative, is to protect **federal** information against compromise to its confidentiality when the federal government makes that information accessible to its suppliers or other non-federal entities, or when the federal government pays for the development and delivery of such information. The revised DFARS definition, unfortunately, creates uncertainty as to "what" information is CDI and

[59] Adding to the challenge is that some Registry categories encompass information types that are subject to specified safeguarding obligations that may differ from SP 800-171. The distinction between CUI "basic" and "specified" refers to the applicable "control level" and is set forth at 32 C.F.R. § 2002.4(j) and (r). As defined, "CUI Basic is the subset of CUI for which the authorizing law, regulation or government-wide policy does not set out specific handling or dissemination controls." 32 C.F.R. § 2002.4(j). DOD's view, as expressed in the FAQs, at Q&A 8, is that only HIPAA data requires additional protection outside the scope of SP 800-171.

[60] This could be accomplished by a change in the regulation, establishing a different "due date" for SP 800-171 protection for CUI categories other than CTI. Or, as a matter of Procedures, Guidance and Information (PGI), DOD could inform components, requiring activities, oversight resources and contracting officers that sufficient compliance, as to "other" CUI categories, is established if the contractor's SSP – now the "110th" requirement of SP 800-171, at 3.12.4 – includes a plan to identify and protect "other" CUI categories.

who makes that determination, and it can be interpreted to reach many forms of **contractor** information that did not originate with, and may never be provided to, the federal government. The DFARS defines CDI to include not only information that is marked or otherwise identified in the contract, but also information that is "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."[61]

The definition of CDI reads (in full text):

> "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/categorylist.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."[62]

The **designation** question is whether it is always the obligation of the DOD component, or requiring activity, to identify and mark *all* information, whether provided to or from a contractor, that is "CDI" and subject to the DFARS and SP 800-171. The plain words of subparagraph (1) suggest that the answer is "yes". However, subparagraph (2) is connected by "or" in a conjunctive usage – meaning that, **apart** from whatever "marked or otherwise identified" information may be subject to (1), anything else that falls within (2) is *also* CDI. And subparagraph (2) is very broad. It is not limited to information provided by the government, or ordered by and furnished to the government. Nor is it limited to information "marked or otherwise identified" in a contract or other agreement. Rather, subparagraph (2) may reach any UCTI or other information that is CUI, if ***any*** of the following activities apply – "collected," "developed," "received," "transmitted," "used" or "stored" – and if the activity is "by or on behalf of the contractor" and "in support of the contract." Multiple uncertainties accompany this phrasing. For illustration –

- If a contractor collects information that fits a CUI definition in a management information system (such as an Earned Value, Estimating or Property Management system), and then it "uses" that information to help manage contract performance, is that use "in support of the contract" such that the DFARS and SP 800-171 apply?

[61] DFARS 252.204-7012 (a).
[62] DFARS 252.204-7012 (a) (emphasis added).

- If a contractor maintains payroll and health benefit records for its employees, or pays a service for these functions, where the nature of the records would fall within one or another CUI category, are they also subject to the DFARS and SP 800-171 because the information was "collected" for the payment of employees and administration of health benefits, which activities are also "in support of" contract performance?

- If a contractor develops intellectual property at its private expense, and a contractor independently "developed" that property so that it could furnish supplies to the Government, is it therefore subject to the DFARS and SP 800-171 where the DFARS -7012 clause is included in the purchase contract, even if the contractor does not furnish the IP to the Government but only uses it to provide a supply or service?

- Similarly, enterprises may develop, again at their own expense, proprietary technical information which would be subject to export controls (a CUI category) but which data the enterprise chooses not to deliver, license or transfer to any customer or to export to anyone. If such information is transmitted from one domestic affiliate to another, or if it is used to build finished articles sold to the Government, under a supply contract with the required -7012 clause, is it then subject to the DFARS and SP 800-171 even where the data is neither exported nor paid for by the Government?[63]

There is less than unanimity among DOD requiring activities as to the responsibilities of their contractors. Some DOD officials insist that it is the job of the requiring activity, or Contracting Officer, in every case, to identify CUI that requires protection on a contract.[64] The regulation, however, can be interpreted otherwise – and in public forums, officials of some prominent DOD components have insisted that "their" contractors *are* responsible to identify and protect CDI even if there is no DOD designation or marking.

As suggested above, DOD can solve this problem by changing DFARS to define "CDI" as only that information designated by DOD as CTI or other forms of CUI which it has furnished to a contractor (or acquired from it) on a contract subject to the -7012 clause. The language might be revised to eliminate subparagraph (2), to read:

> 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/categorylist.html, that requires safeguarding or

[63] The FAQs address but do not resolve this problem, in the author's opinion. FAQ Q&A 10 states: "If the export information is related to the DOD activity, it requires protection as covered defense information." The phrase "related to" is no more helpful to establish the necessary nexus, between the DOD activity and the information in question, than the phrase "in support of" in the -7012 definition that permits such diverse interpretations.

[64] FAQ Q&A 11 states that the requiring activity is responsible to "notify", "mark or otherwise identify" and "[d]etermine" whether CDI is used "in support of the performance of the contract." Unfortunately, the FAQ is *not* the regulation and the language *of* the regulation does not contain the phrasing that places responsibility on the Government. If there were a dispute, a contractor could cite FAQ 11 to justify decisions not to protect certain information – but contractors would prefer clarity in the definition rather than arguments.

dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified, by DOD or on its behalf, as CTI or other form of CUI in the contract, task order, or delivery order;

(2) Provided to the contractor by or on behalf of DOD in the course of ~~support of the~~ performance of ~~the~~ a contract subject to the clause at 252.239-7012; and

(3) Ordered by or on behalf of DOD for delivery by the contractor with direction from DOD that it be identified, designated and marked by the contractor as CTI or other form of CUI.

~~(4) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.~~

C. Methods: What is a Permissible Use of Cloud Services?

The DFARS requires "covered companies" to use the cyber safeguards described by SP 800-171. As recently revised, SP 800-171 identifies 110 security safeguards in 14 families. Some companies subject to the DFARS currently do not have in place an information system that conforms to SP 800-171 and are uncertain, reluctant or even unable to invest to become compliant. The -7012 "Safeguarding" clause is to be included, "without alteration," in subcontracts.[65] DOD has estimated that the DFARS may apply to 10,000 contractors, less than half of whom are small businesses.[66] As the DFARS is flowed down to the defense supply chain, a very large number of contractors, in many tiers, will become obligated to self-assess their capabilities and compare present security to the SP 800-171 safeguards, and to report on any gaps vis-à-vis SP 800-171.[67]

The federal approach to regulate cybersecurity addresses categories of protected information on "covered contractor information system[s]."[68] As defined, this means an "information system that is owned or operated by or for a contractor and that processes, stores, or transmits covered defense information."[69] The attributes of "owned or operated by or for a contractor" qualify the definition of a "covered contractor information system." Thus, the DFARS seeks to safeguard CDI by measures, provided in SP 800-171, to secure "on-premises" systems. Inevitably, the outcome

[65] DFARS 252.204-7012(m).
[66] 80 Fed. Reg. 51740 (Aug. 26, 2015).
[67] DFARS 252.204-7012(b)(2)(ii)(A) requires, for all contracts awarded prior to Oct. 1, 2017, that the contractor notify the DOD CIO office, within 30 days of contract award, "of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award."
[68] *See, e.g.*, DFARS 204.7300 (requiring contractors and subcontractors to safeguard covered defense information that resides in or transits through "covered contractor information systems"). The new FAR clause, "Basic Safeguarding of Covered Contractor Information Systems," at FAR 52.204-21, similarly states "[r]equirements and procedures for basic safeguarding of covered contractor information systems." "Federal Acquisition Regulation: Basic Safeguarding of Contractor Information Systems," FAR Case 2011-020, Final Rule, 81 Fed. Reg. 30439 (May 16, 2016).
[69] DFARS 204.7301 (Definitions); DFARS 252.204-7012(a) (Definitions). *Compare* FAR 52.204-21(a) (a "covered contractor information system" is an "information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information").

will vary from contractor to contractor due to several factors, among them the existing systems and controls, expertise, internal resources, and funds available for such purposes as assessment, monitoring, and improvement. In the commercial world, however, companies are moving from "on-premises" IT to the cloud. To keep pace with the direction and innovation in the commercial sector, federal information security initiatives to protect CUI need not only be "cloud cognizant" but should become "cloud receptive."

Some companies will perceive required improvements to their "on-premises" systems to be time-consuming, resource-intensive, and expensive. Companies will look for affordable, low-risk, non-disruptive solutions that answer the demands of the regulation and satisfy the expectations of higher tier contractors and the government. Until the October 2016 revisions, the DFARS did not address use by DOD contractors of external cloud services.

In an earlier paper, the author wrote that "DOD should clarify the Network Penetration DFARS to authorize companies to safeguard CDI by reliance upon third-party cloud service offerings (CSOs)."[70] That has now occurred. The "Safeguarding" clause of the DFARS now states:

> "If the Contractor intends to use an external cloud service provider to store, process or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program(FedRAMP) Moderate baseline https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment."[71]

FedRAMP offers "federal agencies standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels."[72] The FedRAMP "Moderate" baseline refers to the security controls expected of a cloud service where the information impact of the protected information is deemed "Moderate" under FIPS 199.[73] In its present form, FedRAMP "Moderate" invokes 326 security controls derived from SP 800-53 ("Assessing Security and Privacy Controls in Federal Information Systems and Organizations") which NIST prepared for use by federal agencies (not commercial companies for whom SP 800-171 (with 110 controls) was created). FedRAMP exists to enable adoption and use of cloud

[70] Robert Metzger, White Paper, "Security as a Service: Incorporating NIST 800-171 Requirements Into the Defense Supply Chain," commissioned by Exostar, Sept. 2016, available at http://www.rjo.com/PDF/RSM_ExostarSaaSWhitePaper_09122016.pdf.
[71] DFARS 252.204-7012(b)(2)(ii)(D).
[72] "Guide to Understanding FedRAMP, v.2.0" (Jun. 6, 2014) ("FedRAMP Guide"), available at https://www.fedramp.gov/files/2015/03/Guide-to-Understanding-FedRAMP-v2.0-4.docx. FedRAMP is hosted by the General Services Administration (GSA) and also involves the participation of security experts from the Department of Homeland Security (DHS) and the Department of Defense (DOD).
[73] FISMA defines "information security" in terms of the protection of the "confidentiality," "integrity," and "availability" of information and information systems. 44 U.S.C. § 3544(a)(1(A)). FIPS 199, was developed by NIST to implement the three security objectives of FISMA – confidentiality, integrity and availability. FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," Feb. 2004, at 2.

services by federal Executive branch agencies and departments.[74] While commercial providers may use the FedRAMP process to establish their qualifications – or "authorization to operate" a cloud service on behalf of a federal agency – only some CSPs make FedRAMP-approved cloud services available to contractors, and sometimes there are minimum usage or "seat" requirements that exclude smaller businesses. Moreover, many commercial companies, who happen to be defense contractors, utilize cloud-based services for a wide range of enterprise functions, some of which may require or involve the hosting, transmission or processing of one of the CUI categories.

The DFARS revision informs contractors who are subject to the -7012 "Safeguarding" clause that they may use external cloud services – if they can establish that the CSP "meets security requirements *equivalent to* those established by the Government" for FedRAMP Moderate.[75] It is positive that DOD now accepts use by its contractors of FedRAMP-authorized cloud services. FedRAMP is an established process, accompanied by controls enumerated in SP 800-53 that satisfy federal agencies as to distinctive security issues associated with the cloud instrumentality. But the "window" is not open enough. FedRAMP is an expensive and time-consuming process. While it is improving, through a new "accelerated" process, it can take several years and cost several million dollars for a CSP to receive FedRAMP approval. FedRAMP not only narrows the list of eligible cloud service providers, it makes those services more expensive and less flexible. DOD accepts SP 800-171 for the CDI security of "on-premises" contractor information systems. In contrast, FedRAMP employs a federal-unique review and authorization process and utilizes federal-specific cyber controls and enhancements.

In the commercial world, enterprises of every size and purpose depend upon the functionality **and** security of commercial cloud service providers. Many of these providers make great investment in security and employ "world class" technologies and personnel – and sustain strong security using control strategies and methods that do **not** rely upon NIST SP 800-53. DOD needs to accommodate cloud service providers who employ non-federal security techniques.

- **DOD needs to promptly determine and inform its contractors (and cloud service providers) what is meant by "equivalent" to FedRAMP Moderate, who will make that determination, and what measures (in security or in the cloud service agreement) are sufficient.**

This is just the beginning. Cloud is becoming a prevailing technology. DOD's approach to protection of CDI, and that of other federal agencies as to CUI, must not limit the tens of thousands of affected contractors only to FedRAMP-approved CSPs, even if some programs, uses or information types merit elevated protection. Among recommendations to consider:

[74] "Guide to Understanding FedRAMP, v. 2.0" (Jun. 6, 2014). FedRAMP processes are designed to assist agencies in meeting FISMA requirements for cloud systems and addresses complexities of cloud systems that create unique challenges for complying with FISMA. *Id.*, at 9.
[75] DFARS 252.204-7012(b)(2)(ii)(D) (emphasis added).

- NIST should prepare a "cloud overlay" to SP 800-171. Cloud is all but unmentioned in SP 800-171.[76]

- DOD should create a "dedicated" clause when "external" cloud is used by DOD contractors in the course of their business or to support performance of a DOD contract. The subject now gets just one paragraph, at DFARS 252.204-7012(2)(ii)(D).[77]

- DOD should clarify that the -7012(m) flowdown clause does not apply to enterprise agreements for use of cloud services. Cloud-delivered functions that support business systems may routinely involve access to CUI. The cloud user should not be responsible to DOD for security and reporting, as to such information it shares with a cloud service provider, unless DOD specifically identified that information as CDI and furnished it to the contractor on a contract subject to the DFARS.[78]

D. Adoption: How Can DOD Assist Small Business?

Small businesses form a vital part of the defense supply chain. In 2015, the GAO reported that, in fiscal year 2014, DOD obligated approximately $55.5 billion to small business prime contractors at over 51,000 locations.[79] DOD's Defense Innovation Unit Experimental (DIUx) has been formed to make available to warfighters the capabilities of innovative, non-traditional companies.[80] The defense supply chain not only depends upon smaller businesses, but increasingly seeks them out to leverage technology and agility. The role of small business, and its potential value, can be thwarted if requirements, such as regulatory cyber security safeguards, deter participation in the defense marketplace or drive companies away. At the same time, the national interest in protecting the confidentiality of sensitive technical information does not "stop" at the gates of smaller or venture-stage providers. Adversaries are likely to see the smaller company, or newer defense resource, as an attractive and comparatively more vulnerable target.

Concerns about the ability of small business to accommodate the "Network Penetration" DFARS and SP 800-171 are not new. Responding to an earlier (interim) version of the DFARS, the Office of Advocacy of the Small Business Administration urged DOD to reconsider the impact of the cybersecurity rule on small business, asserting concern that "the cost of compliance with DOD's interim rule will be a significant barrier to small businesses engaging in the federal acquisition process."[81] In the rulemaking that led to the Final DFARS produced on October 21, 2016, DOD

[76] DOD officials have informally insisted that SP 800-171, in its present form, is not sufficient to satisfy the DFARS requirement for "adequate security" when CDI is hosted on an external cloud.
[77] DOD has a separate DFARs, 252.239-7010, that is to be used when cloud is used for an IT service or system operated "on behalf of the Government."
[78] Companies that rely on cloud services for enterprise functions depend upon the availability and security of those systems, but there are many ways, apart from FedRAMP and NIST SP 800-53, that clients can validate, and CSPs can demonstrate, security. Moreover, issues of cloud service "availability" and "integrity" are central to the business model and value proposition of CSPs and do not require federal regulation as to CDI.
[79] GAO, "Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses," GAO-15-777 (Sep. 2015), at 2.
[80] *See* Defense Innovation Unit Experimental (website), https://www.diux.mil/workwithus/ (last visited Feb. 10, 2017).
[81] SBA, Office of Advocacy, Fact Sheet, "Advocacy Urges DOD to Reconsider Impact of Interim Cybersecurity Rule on Small Businesses", undated, *available at* https://www.sba.gov/sites/default/files/DFARS_Fact_Sheet.pdf (last visited Feb. 11, 2017).

received several comments about the cost impact to small business and the concern that small business would be unable to afford the investment and the skilled labor force required.[82] DOD's response was something of a "cold shoulder":

> "While it is understood that implementing the minimum security controls outlined in the DFARS clause may increase costs, protection of unclassified DOD information is deemed necessary. The cost to the nation in lost intellectual property and lost technological advantage over potential adversaries is much greater than these initial/ongoing investments. The value of the information (and impact of its loss) does not diminish when it moves to contractors (prime or sub, large or small)."[83]

DOD insisted that SP 800-171 would benefit small business (i.e., "the medicine is good for you") and promised to "engage across both Government and industry" (i.e., "everyone has to take it") to educate and raise awareness of the importance of CUI and to address implementation of the rule. *Id.* This does not assist small business in compliance or assure prime contractors that they can rely upon the security of their vendors.

Part of DOD's position reflects an expectation that most small businesses should be able to meet SP 800-171 easily.[84] While this proposition may be true for *some* small business suppliers, it does not necessarily characterize the condition (or attitude) of the whole of the large and diverse small business base.[85] There is anecdotal evidence that many small businesses are struggling with DFARS compliance and SP 800-171, and reports that higher tier companies – primes and system integrators – are experiencing uncertainty if not resistance from their smaller supply chain partners.

DOD's goal of information security will not be achieved if it drives small businesses away or it results in empty promises of security or "check the box" exercises. More is needed.

- DOD should actively seek input from the small business community, working with the SBA, and DOD's Office of Small Business Programs. Small businesses may not be heard from in the D.C.-region meetings with large contractors and prominent trade associations. Public meetings at diverse locations would appear advisable.

- Many small businesses are not well informed of what DOD will permit in the achievement of DFARS compliance. Companies can satisfy the DFARS, even if not in full compliance with SP 800-171 by December 31, 2017, if they have a sufficient system security plan and

[82] 81 Fed. Reg. 72987 (Oct. 21, 2016).
[83] Id.
[84] "NIST SP 800–171 was carefully crafted to use performance-based requirements and eliminate unnecessary specificity and include only those security requirements necessary to
provide adequate protections for the impact level of CUI (e.g., covered defense information)." 81 Fed. Reg. 72987 Oct. 21, 2016). "NIST SP 800-171 was written using performance-based requirements, with the intent to not require the development or acquisition of new systems to process, store, or transmit CUI, but enable the contractors to comply using systems and practices they already have in place." FAQs, at Q&A 17.
[85] *See e.g.*, Michael Semmens, "Slow Speed Ahead for Contractor Compliance," *Signal*, Jan. 1, 2016, available at http://www.afcea.org/content/?q=Article-slow-speed-ahead-contractor-compliance (small business compliance with the DFARS cybersecurity standards "could have the unintended consequence of severely diminishing the sector's role in defense contracting").

plan to respond to gaps and mitigate vulnerabilities. DOD and SBA outreach, aided by defense primes, must redouble outreach to inform small and medium-sized businesses how they can combine a SSP and action plan to get "schedule relief."

- DOD should prepare an implementation guide for small business and provide accessible, useful self-assessment tools. DHS now has a Cybersecurity Evaluation Tool (CSET) that, relatively recently, can be used to help businesses assess their cybersecurity against different safeguarding regimes.[86] The current tool may be over-complex for many businesses, and might be simplified. Alternatively, a special tool for small business use, to assist with SP 800-171 compliance, could be created, with assistance from NIST. Small business should be helped to comply without the necessity of hiring expensive outside consultants.

- DOD should create a "facilitation" resource specifically equipped and tasked to help with cyber compliance by small and innovative, non-traditional businesses. A dedicated resource unit, funded by DOD, could provide consultation and guidance to eligible companies. The experience of this unit might prompt DOD to issue implementation guidance (PGI, FAQs), or even to revise the DFARS to address specific small business considerations.

- DOD should include funded tasks for prime contractors to mentor, enable and otherwise assist downstream suppliers to achieve the desired cyber security. Prime contractors have enormous leverage, and contractual privity, with their supply chain. They are in a position to assist their suppliers to achieve security, to qualify and evaluate supplier safeguards, and to implement tools to reduce downstream risk. But these activities have a cost. If DOD intends to make primes responsible for the cybersecurity of their subcontractors, it should pay the primes to assist.

- DOD should make greater use of the NIST Framework.[87] Greater use of the Framework was recently advocated by the Commission on Enhancing National Cybersecurity.[88] At Action Item 1.4.3, the Commission urged regulatory agencies to "harmonize existing and future regulations with the Cybersecurity Framework to focus on risk management – reducing industry's costs of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation." At Action Item 1.5.1, the Commission urges NIST to expand its efforts to help small and medium sized businesses use the Framework.

[86] DHS, ICS –CERT, Assessment Program Overview, at https://ics-cert.us-cert.gov/Assessments.
[87] NIST, "Framework for Improving Critical Infrastructure Cybersecurity", v. 1.0 (Feb. 12, 2014) (the "Framework"), at https://www.nist.gov.cyberframework.
[88] NIST, Commission on Enhancing National Cybersecurity, "Report on Security and Growing the Digital Economy" (Dec. 1, 2016), at https://www.nist.gov/cybercommission.

E. Compliance: What is Sufficient to Demonstrate "Adequate Security"?

How is compliance with the DFARS and SP 800-171 measured? How can companies be confident their measures will pass muster should an investigation follow a cyber incident in which the confidentiality of CDI is compromised?

Companies of all sizes are struggling with these questions. By design, neither the DFARS requirement of "adequate security" nor the SP 800-171 safeguards are prescriptive. Expressly, the DFARS provides a means for companies to "vary from" SP 800-171. Companies may be relieved of obligations for security requirements that are "nonapplicable" and can be approved to utilize an "alternative, but equally effective security measure."[89] NIST specifically acknowledges that non-federal organizations "have specific safeguarding measures in place to protect their information which may also be sufficient to satisfy the security requirements" and that they can "implement a variety of potential security solutions either directly or through the use of managed services, to satisfy security requirements."[90]

The DFARS clause, while imposed on all but COTS suppliers to DOD, is "not structured to require contractor compliance with NIST SP 800-171 as a mandatory evaluation factor in the source selection process."[91] The -7008 "Compliance" clause, required in all solicitations, requires every offeror to "represent" that it "*will* implement" the security requirements of SP 800-171.[92] The -7012 "Safeguarding" clause, however, contains no obligation that a contractor certify that, in fact, it **has** implemented these requirements. Instead, the contractor's obligation is to "provide adequate security" – a term that admits to many potentially different but arguably reasonable interpretations.[93] A contractor's information system shall be "subject to" SP 800-171, but DOD's approach to oversight is restrained:

> "No new oversight paradigm is created through this rule. If oversight related to these requirements is deemed necessary, it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract. *The rule does not require "certification" of any kind, either by DOD or any other firm professing to provide compliance, assessment, or certification services for DOD or Federal contractors.* Nor will DOD give any credence to 3rd party assessments or certifications – by signing the contract, the contractor agrees to comply with the terms of the contract. *It is up to the contractor to determine that their systems meet the requirements.*"[94]

Whether this is the product of "enlightened forbearance" or practical accommodation to the limits of DOD's resources, the companion of this welcome "play in the joints" of the

[89] DFARS 252.204-7012(b)(2)(ii)(B).
[90] SP 800-171, Rev. 1, Ch. 2, § 2.1.
[91] FAQs, at Q&A 21 (but requiring activity "not precluded" from considering compliance with SP 800-171 in the source selection process).
[92] DFARS 252.204-7008(c)(1)(emphasis added).
[93] DFARS 252.204-7012(b).
[94] FAQs, at Q&A 25 (emphasis added).

cybersecurity DFARS is undesirable uncertainty as to how to comply and how to be confident of compliance. This "compliance uncertainty" produces potentially unnecessary costs, as some companies do more than is necessary, especially where drafting issues leave unclear what information must be protected and who is responsible for its designation.[95] Another risk is that companies will promise performance but not even attempt to achieve it.

In fact, "compliance uncertainty" has motivated some responsible participants in the defense industrial base to seek further postponement of the due date for SP 800-171 controls, if only to have more time to figure out what to do. This should be avoided.

The consequences of failure to comply with the DFARS, or fully and effectively implement SP 800-171, are not clear from the regulation. That should be cause for concern among risk managers and compliance officers:

- The DFARS requires rapid reporting of "cyber incidents."[96]
- The PGI for the cyber DFARS instructs DOD components on what to do once a report is received. If requested to do so by the requiring activity, the CO shall "request a description of the contractor's implementation" of the SP 800-171 requirements "in order to support evaluation of *whether any of the controls were inadequate*, or if any of the controls were not implemented at the time of the incident."[97]
- From the PGI, a "reasonable contractor" will conclude that, should a breach occur, there will be an inquiry and examination of the adequacy of controls.
- If there is significant impact from the compromise of CDI resulting from a breach, the inquiry may be "aggressive". A finding of "inadequate" controls could lead to a variety of adverse contractual actions and business consequences.
- Should a basis emerge for suspicion as to contractor "culpability" in the incident, the inquiry may turn into an investigation involving authorities such as the Defense Criminal Investigative Service (DCIS), the Defense Security Service (DSS), the investigative arms of the military departments, the FBI and the Department of Justice.
- In the worst case, the Government could conclude that a contractor made a "false statement" or "false claim" in representing that it would be in compliance with the

[95] Each of the 110 safeguards of SP 800-171 is presented in a single sentence, versus the elaborate treatment that is afforded counterpart controls and enhancements in SP 800-53. Some companies gravitate towards the rigors of SP 800-53 – though these are not required. NIST observes: "To promote consistency, transparency, and comparability, compensatory security measures selected by organizations should be based on or derived from existing and recognized security standards and control sets, including, for example, ISO/IEC 27001 or NIST Special Publication 800-53." SP 800-171, Rev. 1, Ch. 3, n.20. However, DOD cautions contracting officers to ensure that security requirements and assessments are based on SP 800-171 and not to reference a NIST SP 800-53 control. FAQs, at Q&A16.
[96] DFARS 252.204-7012(c).
[97] PGI 204.7303-3(a)(3) (emphasis added).

DFARS, or that payment claims made under the contract were in "reckless disregard" for cybersecurity obligations. These could produce actions under the civil or criminal False Claims Act with exposure to very large penalties and damages, not to mention suspension or debarment.

Nothing in the DFARS, or in the FAQs, or PGI, informs contractors of the consequences of a finding of inadequate controls or deficient implementation. The possibilities include some that would cause concern to any responsible business executive. Beyond the costs of responding to an investigation, companies could face government claims of breach, demands for payment of damages, threat of termination for default, even exposure under the False Claims Act, and suspension or debarment. As is known all too well, the operational or financial impact of a serious cyber breach, where it results in lost confidentiality of sensitive federal records, can be very large – potentially exceeding the limits of calculable damages.

Beyond this "worst case" exposure, companies have to consider the implications of non-compliance, with the cyber DFARS and SP 800-171, as to their eligibility for future contracts or competitive position. On this subject, DOD has provided guidance. The FAQs, at Q&A 21, indicate that a requiring activity may decide to notify an offeror that its approach to protecting covered defense information and providing adequate security in accordance with SP 800-171 "will be evaluated in the solicitation on an acceptable or unacceptable basis." Or, the requiring activity can establish DFARS compliance "as a separate technical evaluation factor" and notify offerors that their approach to providing adequate security "will be evaluated in the source selection process."

Any contractor can experience a cyber breach and the risk of lost confidentiality of CDI cannot be eliminated entirely. But this proposition – however widely accepted – will not remove a defense supplier from scrutiny should it suffer the breach. **Since compliance is ultimately the mitigation not the elimination of breach risk, DOD should develop means to inform and enable its contractors to demonstrate "adequate security" and find "safe harbor" for measures that have been reviewed and accepted:**

- Contractors should not be exposed to sanctions for failure to protect CDI where the government has the obligation to **designate** the information but does not fulfill it. If the requiring activity intends that a contractor take responsibility for designation, this should be clearly specified in the requirements.

- DOD now requires companies to prepare a System Security Plan (SSP). The SSP can serve as the basis for "safe harbor". A "safe harbor" ("acceptable" compliance with the DFARS and SP 800-171) could attach to a contractor's good faith preparation of the SSP and implementation of the "plan of action". This approach does not require submission to or review by DOD – though such would not be excluded and could be required where requiring activities or Program Managers consider necessary for high-value programs.

- DOD could allow contractors subject to the DFARS (including subcontractors receiving the clause as a flowdown) to submit their SSP (and plan) to DOD for review. (A resource would be required.) Absent receipt of DOD objection or notice to take corrective or additional measures, the contractor would be deemed to have "safe harbor" should it implement the plan as described (even if full compliance is not achieved until after Dec. 31, 2017).

- DOD requires its larger contractors to have a "counterfeit electronic part detection and avoidance system [that] shall include risk-based policies and procedures" that address, at a minimum, twelve enumerated system criteria.[98] DOD does not require the covered contractors to submit their system documentation to the Department for review. Instead, the Government reviews and evaluates the contractor's policies and procedures as part of the Contractor Purchasing System Review.[99] The Defense Contract Management Agency (DCMA) has the review responsibility.[100] Drawing on this experience, DOD could call on DCMA to review contractor SSPs. Because of the subject area complexity, and limited DCMA expertise in the area, this approach would require careful and gradual implementation, e.g., initially limited to high-level review of an SSP to confirm that each of the 110 SP 800-171 controls are addressed.

- NIST is developing, for Fall 2017 release, a companion document (SP 800-171A) to SP 800-171 that will provide compliance guidance.[101] The DFARS should enable if not encourage contractors to use the new SP 800-171A assessment methods and to rely upon positive assessment results.

- Higher tier contractors cannot be "guarantors" of the cybersecurity of their supply chain. As to lower tier suppliers, a "safe harbor" should be available where the higher tier contractor (i) flows down the DFARS, as required, (ii) solicits from subcontractors assurance of intent to comply and information regarding the cyber measures in place or planned, and (iii) takes reasonable measures to assure lower tier compliance. The determination of "reasonable measures" would be context–specific and risk-informed. Reasonable measures could be a request for supplier representation of compliance, recognition of third party assessments using accepted tools, satisfaction of supplier due diligence for cyber qualification, or use of a neutral third party for review.

---

[98] DFARS 252.246-7007(c) ("Contractor Counterfeit Electronic Part Detection and Avoidance System").
[99] Id., at 252.246-7007(d)
[100] *See* Defense Contract Management Agency, "Instruction: Counterfeit Mitigation", DCMA-INST 1205 (Jul. 6, 2015), at http://www.dcma.mil/Portals/31/Documents/Policy/DCMA-INST-1205.pdf.
[101] SP 800-171, Rev. 1, Ch. 1, at note 10. SP 800-171A is expected to have a purpose similar to that of NIST SP 800-53A ("Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans"), but, presumably, SP 800-171A will be intended to assist non-federal entities. Reportedly, SP 800-171A will address contractor use of third parties for assessment, and it may further articulate methods for federal oversight and approval. Even if rare, some federal programs will require review of systems security and even federal assessment. In parallel, means should be available to contractors to use third parties, if they so choose, to assess and validate SP 800-171 compliance – and NIST should help to establish the process and controls that third party assessors are to use.

As suggested previously, DOD and the civilian agencies should make greater use of the Framework. On January 10, 2017, NIST released Draft Version 1.1 of the Framework,[102] which includes new content on cybersecurity metrics and measurements. The purpose of the metrics is to "facilitate decision making and improve performance and accountability." In the context of the Framework, these are to assist users in achieving and improving security, and are not "enforcement" tools. The DFARS and the CUI Final Rule contemplate cybersecurity requirements that would affect hundreds of thousands of enterprises. Contract terms will require use of 110 enumerated SP 800-171 safeguards. Achievement of these safeguards, however, is a component of an effective cybersecurity program, not its exclusive measure. DOD and civilian agency regulations can encourage contractors and other non-federal partners to utilize the Framework. Framework principles and processes can be better integrated into the cybersecurity regulatory and contracting scheme.

III. REVISION 1 TO NIST SP 800-171[103]

Revision 1 to SP 800-171, now titled "Protecting Unclassified Information in Nonfederal Systems and Organizations", was released on Dec. 1, 2016.[104] SP 800-171 presents the safeguards that NIST has developed for contractors or other "nonfederal entities" to protect all forms of CUI. DFARS 252.204-7012 obligates DOD contractors to follow SP 800-171 to protect CDI which, as now defined, encompasses all other forms of CUI as well as "operationally critical support" information.[105]

The new revisions to SP 800-171 are not numerous but are important.

In the title and throughout the document, "systems" has replaced "information systems." NIST further explains that "systems" is "defined broadly to include all types of computing platforms that can process, store or transmit CUI."[106] Removal of "information" as a qualifier of systems means that cybersecurity safeguards apply not only to systems that use or host information, but also to other "cyber-physical" systems, such as Industrial Control Systems (ICS) or Supervisorial Control and Data Systems (SCADA) that are vulnerable to cyberattack. NIST explains:

> "This change reflects a more broad-based, holistic definition of information systems that includes, for example: general purpose information systems; industrial and

[102] NIST, "Framework for Improving Critical Infrastructure Cybersecurity", draft version 1.1 (Jan. 10, 2017), *at* https://www.nist.gov/cyberframework/draft-version-11.
[103] An earlier version of this analysis appeared as a LinkedIn Pulse: Robert Metzger, "Key Features of the Newly Released Revision 1 to NIST SP 800-171" (Dec. 21, 2016), at https://www.linkedin.com/pulse/key-features-newly-released-revision-1-nist-sp-800-171-robert-metzger?trk=mp-author-card.
[104] Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf. The baseline version of SP 800-171 was released in June 2015.
[105] "Operationally Critical Support" information is defined and discussed at some length in the FAQs of Oct. 21, 2016. FAQs, at Q&A 4, 5, 13, 14 and 23.
[106] SP 800-171, Rev. 1, Ch. 1, at p.1.

> process control systems; cyber-physical systems; and individual devices that are part of the Internet of Things."[107]

The second key change is the addition of a new derived security requirement, 3.12.4, under the "Security Assessment" family of safeguards, which requires preparation of a System Security Plan:

> "3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems."

In a previous article, the author wrote that "it makes sense that the federal government would expect non-federal holders of CUI to prepare a SSP and a POAM" and that the previous version of SP 800-171 could be considered only "partially complete" because it articulated required controls without an explicit obligation for the affected enterprise to document its security assessment or describe how it intends to satisfy the requirements.[108] Of considerable significance, Revision 1 states, at note 26, that "[t]here is no prescribed format or specified level of detail for system security plans."[109]

Revision 1 does not **require** preparation of a "Plan of Action and Milestones" (POAM). In fact, SP 800-171 uses the formal term, "Plan of Action and Milestones" (POAM), only twice and in neither case is "POAM" either defined or mandated.[110] The apparent explanation is that NIST consciously decided neither to require nor define a POAM, in SP 800-171, because they did not want to cause contractors to believe that they had to "follow the rules" or "obey the process" of SP 800-53 and 800-37 ("Guide for Applying the Risk Management Framework to Federal Information Systems"), both of which apply to exclusively federal agencies and not to contractors.

This does not mean NIST does not expect companies to accompany a SSP with a plan to meet requirements. Revision 1, in several places, links the SSP to an **obligation** to implement unfulfilled requirements identified in that plan. Under "Requirements," at Ch. 3, Revision 1 contains the following statement:

---

[107] SP 800-171, Rev. 1, at p. vi. To note, the DFARS revision in August 2015 included an obligation for contractors to report "malicious software", if detected and isolated. DFARS 252.204-7012(d) (AUG 2015). As defined in the DFARS, "malicious software" means computer software or firmware "intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system." DFARS 252.204-7012(a)(Definitions) (AUG 2015). These provisions, which remain largely unchanged in the present (OCT 2016) DFARS, should be understood to require reporting of "cyber-physical" attacks through "tainted" parts or unauthorized insertion of malicious code upon systems (such as ICS and SCADA) that utilize control firmware and software.

[108] *See* Robert Metzger, "BNA Insights: NIST Proposes Requirements for System Security Plans," 106 Fed. Cont. Rep. 2 (Sep. 12, 2016).

[109] This is in contrast to the draft revision to SP 800-171, circulated for comment in August 2016, which would have required SSPs to conform to NIST SP 800-18 – the guide for developing SSPs for federal information systems. Because it is federal-centric and relies upon security control baselines of SP 800-53, it would have been very costly and burdensome if NIST had invoked the definition of SP 800-18 for SSPs sought from non-federal entities.

[110] The first use is in a mapping from SP 800-53 to security requirement 3.12.4; the second reference is as a potential "tailoring action" if baseline controls require adjustment. SP 800-171, Rev. 1, Table D-12, at App. D, p.47, Table E-4, App. E, p.56.

> "Nonfederal organizations should describe in a system security plan, how the specified security requirements are met *or how organizations plan to meet the requirements*. The plan describes the system boundary; the operational environment; how the security requirements are implemented; and the relationships with or connections to other systems. *Nonfederal organizations should develop plans of action that describe how any unimplemented security requirements will be met* and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format."[111]

This reflects a NIST view that the SSP – now required - encompasses the preparation of a "plan" or "plan of action" to meet the requirements. NIST points forward from the SSP, to the **future** achievement of security requirements, in the new **definition** of "system security plan" which includes the content of "*how an organization plans to meet* the requirements."[112]

Thus, a "system security plan" would not be complete without an included or accompanying plan to meet the security requirements. Revision 1 to SP 800-171 has language that encourages preparation of both the SSP and a POAM, enabling these documents to operate as a "bridge" between the state of a company's security, at the time the SSP is completed, and future compliance:

> "Nonfederal organizations should develop plans of action that describe how any unimplemented security requirements *will be met* and how any planned mitigations *will be implemented*. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format."[113]

This is important language that companies may overlook. Many companies have worried how to demonstrate that they are or will be in compliance and when they are expected to satisfy all the safeguards. The revision to SP 800-171 should be read in conjunction with a related change, to -7012 "Safeguarding" clause which now references the SSP:

> "(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment *or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies* based on an assessed risk or vulnerability. *These measures may be addressed in a system security plan.*"[114]

[111] SP 800-171, Rev. 1, Ch. 3, at p. 9 (emphasis added).
[112] SP 800-171, Rev. 1, at App. B, p. 27 (emphasis added).
[113] SP 800-171, Rev. 1, Ch. 3, at p. 9 (emphasis added).
[114] DFARS 252.204-7012(b)(3) (emphasis added).

The italicized language is newly added, in the Oct. 21, 2016 revision, to the provisions that require contractors to "provide adequate security." The language may be reasonably interpreted to encourage companies to document the SSP and POAM and that they may rely upon these for the time they need to transition from status as initially self-assessed (the SSP) to full compliance with SP 800-171.[115]

On the subject of the CUI Final Rule, NIST now advises that the "CUI FAR clause will address verification and compliance requirements".[116] Today, neither the DFARS nor SP 800-171 include or employ any **government** process or resource for verification or to assess and determine compliance. DOD, at present, disclaims any such requirement. There is no present, government-recognized, available, recommended or required assessment or accreditation methodology for SP 800-171.[117] As indicated above, NIST now is working on SP 800-171A which will provide "assessment procedures to help organizations determine compliance to the security requirements".[118]

IV. CONCLUSION

The CUI Rule, the 'Network Penetration' DFAR and NIST's Special Publication 800-171 work together to serve the crucial public purpose of improving the security of many forms of sensitive but unclassified federal information. Companies also will benefit from measures taken to improve cybersecurity.

Federal law requires agencies to protect certain types of federal information. Those obligations extend to federal contractors and other non-federal entities that have access to that federal information. Injury to both national and corporate interest from cyber exfiltration and other attacks, is well-established. Federal measures to improve supply chain cybersecurity are urgent and should not be delayed. Achieving better cybersecurity for the federal supply chain is a continuing challenge to address evolving threats in a dynamic environment.

Regulations and contract requirements are imperfect, but necessary means to achieve cybersecurity goals. Pursuit of compliance can prove costly and disruptive and certitude elusive. Those responsible for the regulations, standards and contractual implementation must consider whether their actions are proving effective and if the results justify the costs. They must be informed about how industry partners perceive and respond. Regulations and implementation

[115] As discussed above, documentation of the SSP and POAM, and good faith effort to implement the measures called for in the POAM, will assist companies to achieve and sustain adequate security and to demonstrate compliance to government reviewers, auditors or investigators in the event of inquiry or investigation following a breach. Moreover, companies are encouraged to prepare these documents for competitive purposes. DOD's FAQs indicate that a requiring activity may evaluate the approach of offerors to protecting CDI and providing adequate security and that compliance with DFARS 252.204-7012 can be made an evaluation factor. FAQs, at Q&A 21, 34.
[116] SP 800-171, Rev. 1, at p. v.
[117] In the FAQs, DOD comments that companies may choose to seek outside assistance in determining how best to implement SP 800-171. "But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171." FAQs, at Q&A 25.
[118] SP 800-171, Rev. 1, at p. v.

need to evolve on an informed basis. Measures can be taken to better inform industry of what is expected, to accommodate and assist industry where pressure points are identified, to avoid excess cost, and to mitigate dysfunctional consequences such as exclusion of small and innovative businesses.

---

[i] Robert S. Metzger, rmetzger@rjo.com, heads the Washington, D.C., office of Rogers Joseph O'Donnell, PC, a boutique law firm specializing in public contracts. He is a Vice-Chair of the ITPS Cybersecurity Acquisition & Supply Chain Assurance Committee. Bob was named a 2016 "Federal 100" awardee by *Federal Computer Week* for his contributions to cyber and supply chain security. This article reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated. Certain portions of this White Paper appear in the author's previous article, "*Cyber Protection of CDI: Changed Requirements, New Methods, More Questions*", Bloomberg BNA Federal Contracts Report, 107 Fed. Contr. Rep. 217 (Feb. 28, 2017).