Security as a Service

Incorporating NIST 800-171 Requirements into the Defense Supply Chain

White Paper

Commissioned by

EXOSTAR®

Written by: Robert S. Metzger*

September 2016

Contents

Introduction

The Department of Defense (DoD) now requires all of its contractors to protect "Covered Defense Information" (CDI).[1] The Network Penetration Defense Federal Acquisition Regulation Supplement (DFARS) requires safeguarding of four types of CDI, including "controlled technical information" and "export control information."[2] The DFARS requires "covered companies" to use the cyber safeguards described by the National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-171,[3] which NIST created specifically for commercial companies who do not operate "federal information systems" but who receive or create CDI to perform defense contracts. NIST SP 800-171 identifies 109 security safeguards in 14 families. These safeguards were developed to protect all forms of "Controlled Unclassified Information" (CUI), including CDI.[4] Today, they are imposed by regulation only upon DoD contractors. Federal civilian agencies have not yet issued acquisition regulations, like the Network Penetration DFARS, to require contractors to safeguard CUI. But they are in the works.

Many companies subject to the DFARS currently do not have information systems in place that conform to the safeguards of SP 800-171 for the CDI they receive, create, or transmit. Even though SP 800-171 describes safeguards as high-level goals, and NIST intends flexible application, some companies are reluctant or even unable to invest to become compliant with the new safeguards. The problem is particularly acute among mid-size and smaller companies for whom DoD may not be a dominant customer. DoD faces a fundamental dilemma. It has powerful reasons to extend cyber safeguards "down" and "across" its supply chain to where controls are weakest today. Suppliers who are most vulnerable to compromise are the least equipped to adopt effective protective measures.

The Network Penetration DFARS and SP 800-171 impose cyber safeguards to protect CDI in the information system(s) operated by any defense supplier that receives a contract or subcontract subject to the new requirements. Every contractor that takes a contract with this DFARS is subject to an

---

[1] The applicable regulation is the "Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services" (DFARS Case 2013-2018), Interim rule, (hereafter, "Network Penetration DFARS"). The Network Penetration DFARS was first promulgated on Aug. 26, 2015. 80 Fed. Reg. 51739. The Interim rule was revised by a subsequent promulgation. 80 Fed. Reg. 81472 (Dec. 30, 2015).

[2] The four types of CDI are ''controlled technical information'' (with military or space application), critical information (operations security), export controlled information, and ''[a]ny other information'' that requires safeguarding or dissemination controls pursuant to ''laws, regulations, and government-wide policies" (DFARS 204.7301 (Definitions)). The first of these types, "controlled technical information," corresponds to what was controlled as "Unclassified Controlled Technical Information" (UCTI) under an earlier regulation. "Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information," (DFARS Case 2011-D039), Final rule, 78 Fed. Reg. 69273 (Nov. 18, 2013).

[3] NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," June 2015, *available at* http://dx.doi.org/10.6028/NIST.SP.800-171. In August 2016, NIST released a proposed "Revision 1" to SP 800-171. Comments are due on Sep. 16, 2016. The proposed revision is available at http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-171-Rev-1.

[4] Pursuant to Executive Order 13556, Nov. 4, 2010, the National Archives and Records Administration (NARA) acts as the "executive agent" to produce a new Federal Acquisition Regulation (FAR), of general application, to govern designation, dissemination controls, and safeguards for all forms of "Controlled Unclassified Information" (CUI). *See* "Controlled Unclassified Information" Proposed rule, 80 Fed. Reg. 26501 (May 8, 2015). NARA maintains a "Registry" that identifies 23 categories and 82 subcategories of CUI. "Controlled Technical Information" and "Export Control" are two of the 23 categories. The Registry is available at https://www.archives.gov/cui/registry/category-list.html.

immediate requirement to provide "adequate security" for CDI and contractors must report "cyber incidents" within 72 hours of discovery (DFARS 252.204-7012(b)). In addition, a company that receives a contract subject to the new DFARS must report to the DoD Chief Information Officer (CIO) – within 30 days of contract award – any security requirement specified by SP 800-171 "not implemented at the time of contract award" (DFARS 252.204-7012(b)(2)(ii)(A)). Full compliance with SP 800-171 is not required until Dec. 31, 2017 (DFARS 252.204-7008(c)(1)). The deferred date offers contractors and their supply chains time to achieve full compliance, as well as an opportunity for the DoD to improve the DFARS and to address serious questions as to whether it will succeed with its important, intended purpose.

The DFARS clause is to be included, "without alteration," in subcontracts (DFARS 252.204-7012(m)). DoD has estimated that the DFARS may apply to 10,000 contractors, less than half of whom are small businesses. 80 Fed. Reg. 51740 (Aug. 26, 2015). A large majority of these 10,000 contractors, and a very sizable number of small businesses, will become subject to the new DFARS, and obligated to protect CDI, by operation of the mandatory "flowdown." The DFARS obligates every covered contractor to "implement information systems security protections."

Thus, as the DFARS is flowed down to the defense supply chain, a very large number of contractors, in many tiers, will become obligated to identify where CDI resides in their information systems, to self-assess their capabilities and compare to the SP 800-171 safeguards, and to report on any gaps vis-à-vis SP 800-171. All of this effort is directed to "on-premises" information systems (i.e., those hosted by, or operated for, individual companies). Some companies will perceive compliance to be time-consuming, resource-intensive, and expensive. Many 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.

Assessment and Recommendations

The DFARS imposes obligations on companies to identify and protect information, irrespective of company size or how much of its business is for DoD. Just to complete the initial compliance assessment may require the use of expensive outside resources. Thus, some will object that DoD rules impact information systems across an entire enterprise, even where DoD work is a small fraction of their overall business. Companies can isolate the government information into separate domains, but this may be an impracticable option for many among the thousands of companies in the DoD supply chain. Unfortunately, in order to retain DoD business, there will be companies who promise adherence without taking the expected measures to protect the covered information and information systems.

There are important national objectives to be served by improving the safeguards of sensitive but unclassified information created, used, and transported by government contractors. Unauthorized access to such information and its "exfiltration" have proven harmful to the national interest and to the business interests of companies who suffer such attacks. The government's objective in the use of its regulatory and acquisition authority to improve contractor security is sound. The basic control architecture of SP 800-171 has much to recommend it. NIST took great care to extract key principles of security controls that can be adapted and employed by many different kinds of commercial companies. However, the success of these measures must be judged by their results.

The DoD supply chain consists of thousands of participants. Companies at every tier of the supply chain create and use information that merits protection. Adversaries know to direct their threats to lower tier suppliers. For the federal initiative to succeed, cybersecurity practices must improve *throughout* the supply chain – and not just among the "high tiers" where security is likely to be strong already. Specifically, security must be improved among the many companies who, by reason of size, limited resources, or poor present security, have the most reasons to object to the difficulty of the DFARS and SP 800-171. **The Government should enable and encourage all suppliers to achieve and sustain security without reliance upon safeguards developed specifically for federal information systems**.

The federal approach to regulate cybersecurity affects "covered contractor information system[s]."[5] As defined in the DFARS, this means an "information system that is owned or operated by or for a contractor and that processes, stores, or transmits covered defense information."[6] 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. **The present focus on security measures for "on-premises" systems merits reconsideration**. Inevitably, the outcome will vary from contractor to contractor due to several factors, among them the expertise, internal resources, and funds available for such purposes as assessment, monitoring, and improvement. **In the commercial world, the paradigm is shifting away from "on-**

[5] *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).

[6] 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").

premises" IT to the cloud. Federal information security initiatives to protect CUI held or used by commercial companies must be "cloud cognizant" and "cloud receptive."

There is a better way – which will be more *affordable* and *accessible* – for companies to *improve* security beyond what will be achieved by measures focused upon "on-premises" systems.

- *DoD should clarify the Network Penetration DFARS to authorize companies to safeguard CDI by reliance upon third-party cloud service offerings (CSOs)*. Outside the federal environment, innumerable private companies routinely make sensitive and regulated data available to Cloud Service Providers (CSPs) and execute cloud-based applications using that data. The security commitment of the CSP and expectations (and rights) of the cloud service client are expressed in the cloud service contract and accompanying Service Level Agreements (SLAs). The Network Penetration DFARS should identify minimum, acceptable provisions for cloud service contracts and for SLAs when a covered defense supplier entrusts CDI to a third-party cloud resource.

- *NIST should evaluate whether an overlay to SP 800-171 is needed to deal with cloud-unique security issues*. Cloud solutions raise certain security issues not present for "on-premises" information systems.[7] Some federal officials worry that the cloud is a concentrated and attractive target to potential adversaries. Reasons include large volumes of information in a multi-tenant environment, doubts as to isolation of virtual domains, and potential vulnerabilities through public internet access and connection. These considerations merit examination of an "overlay" to SP 800-171 to address security issues distinct to cloud solutions.[8]

- *Cloud Service Offerings to protect CDI and CUI should accommodate multiple assessment and accreditation regimes and not demand federal-centric process or methods.* A guiding principle should be maximum reliance upon commercial best practices for cloud security. There are multiple sources and standards for process and controls successfully used by CSPs worldwide. Federal security objectives do not dictate insistence that its *commercial contractors* adhere to complex, cumbersome, and costly processes that the federal government has chosen to impose upon federal agencies when they perform federal missions using cloud services.

- *NIST can assist to recognize and validate commercial standards and best practices for cloud security*. NIST already accepts the proposition that the federal interest in "confidentiality" of CUI can be satisfied by means other than reliance upon the controls of SP 800-53 created for

[7] As recognized in the ISO/IEC International Standard 27017 for cloud services, cloud computing has its "own types of risk sources, including threats and vulnerabilities, which are derived from its features, e.g., networking, scalability and elasticity of the system, resource sharing, self-service provisioning, administration on-demand, cross-jurisdictional service provisioning, and limited visibility into the implementation of controls. Annex B provides references that give information on these risk sources and associated risks in the provision and use of cloud services." [at 4.4]

[8] NIST should involve stakeholders to determine what measures are necessary – and to recognize the accomplishments of the private sector. Security issues are regularly and successfully addressed by many world-class cloud service providers. They routinely employ advanced technical and operational means to reduce vulnerability, expedite threat detection, and accelerate response. Leading cloud providers can hire and retain top human resources, and employ advanced technical methods, not usually replicable by individual companies.

"federal information systems."[9] One of the "basic assumptions" of SP 800-171 is that nonfederal organizations have specific safeguarding measures in place (independent of SP 800-171) to protect their information that "may also be sufficient to satisfy the CUI security requirements." [10] SP 800-171 recognizes that "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 27001/2 or NIST SP 800-53."[11] NIST can assist both industry and government by examining alternative cloud-specific security regimes, such as ISO/IEC 27017, or the Cloud Security Alliance (CSA) Cloud Controls Matrix. NIST can help articulate what should satisfy federal agencies when contractors rely upon cloud for security.[12]

DoD should recognize commercially-provided, cloud-enabled ***Security as a Service*** as a secure, scalable, flexible means for its *entire* supply chain to meet and exceed the objectives of SP 800-171 safeguards and to sustain security in a dynamic environment. Once refined through DoD's leadership and informed by the experience of the defense supply chain, these strategies and methods can then be employed for protection of all forms of CUI when the civilian agencies move to require protection of CUI.[13]

- *Security as a Service* is a form of "Software as a Service" (SaaS), one of the three cloud service delivery models recognized by NIST SP 800-145.[14] Defense contractors with CDI are prospective customers of CSPs who offer *Security as a Service*. A contractor, for illustration, would identify "Covered Defense Information" that it uses to provide a product to, or perform a service for, DoD. It would contract with a CSP to move the CDI data to the cloud. The CSP would become contractually responsible to host and safeguard the data and to manage access and use by the customer. The cloud security provider would address all objectives of NIST SP 800-171 and add other measures as federal agencies may determine are necessary to address distinct security risks of cloud computing. The scope of *Security as a Service* can vary, from a baseline of secure hosting to higher value services that include elevated identity and access management (IAM), improved authentication methods, supply chain risk mitigation, and information rights management (IRM).

---

[9] SP 800-171 states that organizations "*can* use Special Publication 800-53 to obtain additional, non-prescriptive information related to the CUI security requirements." NIST SP 800-171, Ch. 3, at p.8 (emphasis added). The use of the word "can" – as distinct from "shall" – means organizations may elect, but are not obligated, to use SP 800-53.

[10] *Id*., Ch., 2, ¶2.1, at p.5.

[11] *Id.,* n.21, at p.8. Essentially identical language is retained in the proposed Revision 1 to SP 800-171.

[12] For cloud, use of commercial alternatives should not be allowed only to "compensate for the inability to satisfy a particular requirement," as suggested in the present wording of SP 800-171. *Id.*, Ch. 3, at p.8. Instead, to facilitate cloud security, the objective is to establish *equivalent* status for protection of CUI, as well as process and controls built upon alternative standards and practices. Eventually, "reciprocity" should be encouraged among international organizations in cloud and IT system security standards and practices.

[13] A final FAR rule, "Basic Safeguarding of Contractor Information Systems," became effective on June 15, 2016. 81 Fed. Reg. 30439 (May 16, 2016). This rule applies to "Federal contract information" (FCI) (which is very broadly defined), though the focus of the rule is to protect "information systems" rather than proscribed information types. It applies to all acquisitions, except commercial off-the-shelf (COTS) solutions, and articulates 15 safeguards, derived from SP 800-171. The new FAR will affect virtually every company (and many other authorized recipients) who do business with any federal agency – civilian or military. This rule also should be made "cloud friendly."

[14] NIST SP 800-145, "The NIST Definition of Cloud Computing," Sep. 2011, *available at* http://dx.doi.org/10.6028/NIST.SP.800-145.

- Commercial use of any public cloud service is accomplished by a service contract and accompanied by an SLA. The requirements of that contract and the terms and conditions of the SLA offer means to allocate risks and responsibilities between the CSPs and DoD contractors who purchase *Security as a Service*. There are "best practice" norms for the content of cloud service contracts and SLAs. For *Security as a Service,* DoD should identify "minimum" or "recommended" terms (if necessary) to protect DoD's interests. CSPs regularly employ sophisticated and continuous monitoring and demonstrate rapid incident response and resilience. Federal interests in these areas may be satisfied by prevailing commercial practices. If needed, DoD can identify additional measures it expects in cloud service contracts and SLAs when a defense contractor satisfies the DFARS using cloud *Security as a Service*.[15]

- Among the most important of the SP 800-171 safeguards required by the DFARS is requirement (3.5.3) that companies must "[u]se multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts." CSPs can provide strong methods to limit access to data secured in the cloud. Comparable measures are not likely to be implemented for "on-premises" systems and may not be affordable. For *Security as a Service*, CSPs can provide government contractors with affordable, sophisticated IAM and IRM tools. Properly implemented, these improve assurance against unauthorized access and offer positive, "life of the data" controls over information dissemination and use. IRM, in particular, offers "defense in depth" because rights to view or utilize information can be revoked should unauthorized access occur, regardless of where the associated document travels.

The basic obligation imposed by the DFARS on companies who have CDI is to provide "adequate security" (DFARS 252.204-7012(b)). The regulation defines "adequate security" as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information" (DFARS 252.204-7012(a)). To provide "adequate security," contractors must use protections that, "at a minimum," meet the requirements of SP 800-171 (DFARS 252.204-7012(b)(1)). However, *beyond* this obligation, contractors must also apply "other information systems security measures" when "required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability" (DFARS 252.204-7012(b)(2)). Beyond the top-tier defense contractors, few companies possess the resources or knowledge to assess and respond to changes in the dynamic threat environment. "Adequate security" is more likely to be achieved if companies can move their CDI (and proprietary business information, if they choose) to the cloud, where CSPs can leverage continuing investments in security and employ elite resources to protect many users against evolving threats. Continuing security can hardly be assured if the outcome is left to the individual decisions of thousands of companies affecting only their "on-premises" IT systems. "Adequate security," even by the DFARS measure, can be delivered affordably as a cloud service using methods and technologies that exceed what most companies can achieve individually. A *Security as a Service* cloud solution, subject to reasonable requirements to protect CDI in a cloud environment, is in everyone's best interest to ensure compliance and security throughout the contractor supply chain.

[15] DoD-mandated obligations can be informed by NIST judgments about the adequacy of process and controls of alternative security regimes. DoD should refrain from imposing unnecessary obligations on commercial CSPs that would dilute the economic advantages that accompany multi-tenant operation of cloud infrastructure.

Supporting Analysis

The Threat

There is ample evidence that U.S. adversaries have preyed upon the defense supply chain to "exfiltrate" valuable technical and operational information. Similarly, foreign states and foreign business rivals have circumvented export control restrictions by cyberattacks that have gained unauthorized access to controlled technical information. Too often, where unencrypted information has been stolen by an attack, or otherwise made accessible to unauthorized persons, means have not been available to recover the information or rescind privileges to access and use of the information.

DoD relies upon its defense supply chain to produce and support systems and to provide services. It entrusts its suppliers with sensitive technical and operational information for those purposes and pays them to create and exploit such information. DoD shares "Covered Defense Information" (CDI)[16] with its principal suppliers, and CDI is created by those suppliers for DoD. Those suppliers, in turn, must further share and receive CDI with their supply chain – even parts of the supply chain whose business is dominated by commercial rather than government customers. Cyber "raids" upon the supply chain have weakened our defense and enabled rivals to use stolen information to narrow or even eliminate the technical advantage for which U.S. taxpayers have paid billions. This is a persistent and evolving threat. The importance of an effective response is growing. For the U.S. to succeed with its "Third Offset Strategy," intended to exploit areas where the U.S. has asymmetric advantages in unique technologies, protection of critical technical information is essential.

DoD's *Better Buying Power 3.0* states plainly that compromise of unclassified controlled technical information "can significantly degrade U.S. technological superiority by saving an adversary time and effort in developing similar capabilities or countermeasures."[17] Where contractor information systems host sensitive DoD technical information that is vulnerable, company proprietary information and trade secrets are likely to be similarly exposed. Hence, the security interests of DoD and its contractors "dovetail," are complementary in significant respects. An objective common to the federal government and its contractors is to improve security and better protect the confidentiality of information. Means to accomplish this objective should be accessible, affordable, and effective. Insistence upon federal-specific security measures can impose burdens and costs with undesirable consequences. Some commercial sources could exit the supply chain. Moreover, commercial methods may equal or even improve upon the federal-specific strategies and controls.

DoD's Initiatives to Protect Information

DoD first wielded its acquisition authority in 2013, when it obligated contractors to protect "Unclassified Controlled Technical Information" (UCTI). These obligations were expanded and refined in 2015, by the Network Penetration DFARS, which makes DoD contracts subject to DFARS 252.204–7012 (*Safeguarding Covered Defense Information and Cyber Incident Reporting*). This "Safeguarding" clause imposes several obligations on defense contractors. It states:

---

[16] CDI is unclassified information that is (A) Provided to the contractor by, or on behalf of, DoD in connection with the performance of the contract; or (B) Collected, developed, received, transmitted, used, or stored by, or on behalf of, the contractor in support of the performance of the contract. DFARS 204.7301.

[17] See "Implementation Directive for Better Buying Power 3.0 – Achieving Dominant Capabilities through Technical Excellence and Innovation," Apr. 9, 2015, at 5, *available at* http://www.acq.osd.mil/fo/docs/betterBuyingPower3.0(9Apr15).pdf.

> "The Contractor shall provide adequate security for all covered defense information [CDI] on all covered contractor information systems that support the performance of work under this contract."

For contractor information systems, the "Safeguarding" clause requires, "at a minimum," implementation of the security requirements of NIST SP 800-171, and this must be done "as soon as practical, but not later than December 31, 2017." Flowdown of the "Safeguarding" clause is required – "*without alteration*" [emphasis added] – to subcontractors who receive or host CDI (DFARS 252.204-7012(m)(1)).

The Network Penetration DFARS requires all DoD suppliers to comply with minimum cybersecurity standards for "Covered Defense Information" (CDI). DoD contractors now are receiving solicitations, which they must flowdown to all levels of their supply chain, requiring that they safeguard CDI in using SP 800-171 safeguards. As initially promulgated on Aug. 26, 2015, in 80 Fed. Reg. 51739, the DFARS could be understood to require any contractor, where the clause at DFARS 252.204-7008 was present, to be in full compliance with SP 800-171 requirements at proposal submission. Many defense contractors objected, surprised at these requirements and uncertain about how to respond. Some expressed doubt that they could bid on solicitations with requirements they had not met. Recognizing industry resistance, and fearing a breakdown in the acquisition system, DoD revised the rule on Dec. 30, 2015. It postponed until Dec. 31, 2017, the date by which companies must be in full compliance with SP 800-171.

About 1,200 companies are prime contractors or sub-contractors who have enough DoD business to be subject to all or some of the federal Cost Accounting Standards. 79 Fed. Reg. 26105 (May 6, 2014). As noted above, DoD has estimated that as many as 8,800 more companies (for a total of 10,000) are defense suppliers who possess or use one or another form of CDI. To fulfill DoD's objectives, and to comply with the DFARS, *every one of these companies* must have cyber safeguards in place to protect CDI, and those measures must conform to NIST SP 800-171, no later than Dec. 31, 2017.

When a company accepts a contract (or subcontract) that contains the mandatory clause at DFARS 252.204-7012, there is an immediate obligation to provide "adequate security" for all CDI on all covered contractor information systems that support the work under the contract. Moreover, the "Safeguarding" clause, as revised on Dec. 30, 2015, requires that companies notify the DoD Chief Information Officer (CIO), within 30 days of award of any contract subject to the DFARS, of any security requirement of NIST SP 800-171 that is not satisfied at the time of award. Even though full compliance is not required until the end of 2017, the DFARS imposes prompt obligations both to assess controls and report cyber events. Nonetheless, the interval before expected full compliance offers both industry and government the opportunity to clarify and facilitate successful achievement of enhanced information security.[18]

[18] On August 2016, NIST released a proposed "Revision 1" to SP 800-171, *available at* http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-171-Rev-1. The most important change is the addition of guidance on use of "system security plans" (SSPs) and "plans of action and milestones" (POAMs) to "demonstrate the implementation or planned implementation of CUI requirements by nonfederal organizations." Id., "Notes to Reviewers," at p. v. In explaining the new requirement, the proposed revision speaks to "planned implementation or mitigations." Id., Ch. 3, at p. 8. This language recognizes that companies will need time to meet SP 800-171 requirements.

Industry's Response & Concerns

DoD's largest contractors likely already have systems in place that meet SP 800-171. However, "flowdown" obligations make DoD prime contractors responsible for cyber compliance of sources. Thus, higher tier contractors have strong interests in assurance that all participants in their supply chain are able to protect CDI. Valuable DoD technical information needs protection, regardless of where it resides within the supply chain.

There is no definitive evidence of how the defense supply chain is responding to the cyber obligations of the "Network Penetration" rules. Anecdotal information suggests that some larger companies are struggling to reconcile the NIST SP 800-171 with existing security methods. Many companies are responding cautiously as they seek ways to comply that are both practical and affordable. Smaller companies in particular are taking a "wait and see" course. There is risk that some companies will respond to new obligations as mere exercises in documentation (i.e., "check the box"). The DFARS relies upon self-assessment, self-attestation, and self-improvement by defense contractors. The DFARS is unaccompanied by required third-party security assessments or continuous monitoring. There exist at present neither method nor resources for accreditation to SP 800-171 requirements. The absence of such measures may tempt some companies to "claim" safeguards that do not exist. If burdens to compliance can be reduced, there will be less incentive to evade requirements, and less risk that suppliers will choose to exit the defense supply chain rather than shoulder the new cyber requirements.

DoD has a daunting challenge. It wants to improve access to the dynamism, diversity, and technology of commercial sources. But mandatory DoD-specific cyber controls can discourage participation by agile commercial sources. DoD wants to retain in the defense industrial base the small, specialized providers who can play pivotal roles on programs irrespective of their size. Yet those smaller suppliers are comparatively more exposed to cyber threats than larger sources at higher tiers. DoD depends upon its supply chain to design, develop, manufacture, and support systems, and for many mission-essential services – all of which, inevitably, lead DoD to create, share, and receive increasing volumes of sensitive technical information. **DoD should act to enable – not frustrate – its entire supply chain to protect the confidentiality of each form of "Covered Defense Information**." **This can be done by lowering the barriers to the use of cloud services to secure CDI and other forms of information.**

Using Cloud Services to Protect "Covered Defense Information"

As configured today, the Network Penetration DFARS and SP 800-171 inform defense contractors of the measures that they must take to make their company-hosted ("on-premises") *information systems* conform to NIST cybersecurity safeguards.[19] Neither the "Compliance" solicitation clause (DFARS 252.204-7008) nor the "Safeguarding" contract clause (DFARS 252.204-7012) contemplate contractor use of cloud-services to address the security requirements. (The "Compliance" clause makes no reference to the cloud whatsoever.)

[19] For covered contractor information systems, the security requirements are those provided by NIST SP 800-171 *or* "[a]lternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO" (DFARS 252.204-7012(b)(1)(A), (B)). Many commercial companies will have built their security measures without recognition of NIST publications. From a compliance standpoint, it can be challenging for companies subject to the DFARS to be confident their choice and implementation of safeguards is sufficient. The "high level" approach to safeguards, reflected in NIST SP 800-171, contributes to this uncertainty.

The "Safeguarding" clause only references cloud computing in the context of information systems that are part of an IT service or system "operated on behalf of the government" (DFARS 252.204-7012(b)(1)(i)(A)). This language refers to a "federal information system" (i.e., one "used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency").[20] As to such systems, the clause states that cloud computing services shall be subject to the security requirements specified in another DFARS, 252.239-7010. The -7010 clause invokes cloud security requirements "with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG)" (DFARS 252.239-7010(b)(2)). These are requirements dictated by the Defense Information Systems Agency (DISA), for *military* use of the cloud.[21]

Upon examination, it is clear that the Network Penetration DFARS invokes specific cloud security requirements – namely, the DISA-authored SRG – *only* for cloud services that a contractor provides as a *federal* information system. These DFARS cloud security requirements do not apply to *contractor* information systems that process, store, or transmit Covered Defense Information. **The Network Penetration DFARS contains no cloud-specific security requirements governing contractor use of third-party cloud service offerings that may involve access to, use, or transmission of CDI.**

Similarly, the safeguards of NIST SP 800-171 today contain no content specifically tailored to cloud security where contractors entrust CDI (or CUI) to the cloud. The word "cloud" appears only once in the entire Special Publication. Although many, if not all, of the stated controls have relevance to cloud services, *none* of the 109 basic and derived security controls enumerated by SP 800-171 are specific to or tailored for "cloud."[22] NIST prepared SP 800-171 to address "on-premises" IT systems (i.e., those hosted by the contractor). The subject is not addressed directly in the DFARS, nor in SP 800-171, meaning that CSPs and potential customers are unsure what is needed to satisfy DoD's security requirements if contractors utilize the public cloud for storage, access, and processing of CDI (or CUI). The uncertainty discourages suppliers from using cloud solutions to meet the objectives of the DFARS.

Enabling *Security as a Service*, using third-party public cloud services, is an achievable, affordable, and effective way for federal suppliers at every tier to safeguard Covered Defense Information and Controlled Unclassified Information. DoD and other federal agencies are principal beneficiaries if more organizations with sensitive federal information can utilize the cloud for security.

Cloud Security for Federal Information Systems

The federal government has embraced a "cloud first" policy.[23] DoD also is increasing its use of cloud services. For civilian agencies, the Federal Risk and Authorization Management Program (FedRAMP)

[20] 40 U.S.C. § 11331 (FISMA); see also FIPS-199 (Appendix A: Terms and Definitions), *available at* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[21] The SRG is available at http://iase.disa.mil/cloud_security/Pages/index.aspx. In addition, the "Safeguarding" clause states that a contractor, where utilizing a cloud as a federal information system, must maintain government data in the United States absent approval of the Contracting Officer (DFARS 252.239-7010(b)(3)).

[22] The cloud "risk sources" identified in ISO/IEC International Standard 27017, *supra* n.7, are not addressed specifically by any of the 109 basic and derived controls of SP 800-171.

[23] "Federal Cloud Computing Strategy," The White House, Feb. 8, 2011, *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

process is employed to assess and then authorize CSPs to host sensitive federal data or perform federal information system functions on behalf of federal agencies.[24]

The Federal Information Systems Modernization Act (FISMA), 40 U.S.C. § 11331, places a legal obligation on federal agencies to "provide information security protections" for the confidentiality, integrity, and availability of certain federal information. FedRAMP was formed for federal agencies to have the assurance necessary to satisfy the FISMA statute and related obligations when agency functions are moved to the cloud. FedRAMP adds security requirements for cloud authorization, beyond controls that otherwise would be required for "federal information systems" by NIST SP 800-53 r4 – the NIST Special Publication that is a comprehensive catalogue of controls and enhancements that federal agencies follow to fulfill FISMA requirements.[25]

When DoD uses the cloud, it goes beyond how FedRAMP is implemented by civilian agencies. Through the SRG, DoD adds more obligations that must be met by CSPs for cloud service offerings, depending on the nature of DoD information involved.[26] DISA presently identifies four discrete "information impact levels" – Level 2 ("publicly releasable data"), Level 4 ("unclassified sensitive data"), Level 5 ("unclassified national security data") and Level 6 ("secret or secret NSS").[27] Even for Level 2 ("publicly releasable data"), the SRG requires a FedRAMP-approved public cloud offering. For Levels 4 and 5 – which overlap with "Covered Defense Information," as defined in the Network Penetration DFARS – the SRG requires "FedRAMP +" security control enhancements.[28] In addition, when the cloud is to be used to host these forms of unclassified defense information, DISA must issue a DoD Provisional Authorization (PA).[29]

---

[24] The Federal Risk and Authorization Management Program (FedRAMP) is described as offering "standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels." *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).

[25] NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, *available at* http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[26] *See* "Best Practices Guide for Department of Defense Cloud Mission Owners," v.1.0, Aug. 8, 2015, at 8, *available at* http://iasecontent.disa.mil/stigs/pdf/unclass-best_practices_guide_for_dod_cloud_mission_owners_FINAL.pdf,

[27] *See* Department of Defense, "Cloud Computing Security Requirements Guide," Version 1, Release 2, Mar. 18, 2016, at 15-19, *available at* http://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r2.pdf. The SRG assigns various "impact levels" according to information sensitivity. While similar in purpose, the SRG is not entirely aligned with how the four categories of "Covered Defense Information" are treated in the Network Penetration DFARS. The SRG states that Level 4 "accommodates CUI or other mission critical data" and describes CUI as "information the Federal Government creates or possesses that a law, regulation, or Government-wide policy requires, or specifically permits, an agency to handle by means of safeguarding or dissemination controls." SRF, § 3.2.4, at 18. This definition of CUI is essentially identical to that used by NIST in SP 800-171, Ch. 1, n.4, at p.1. The SRG also identifies as CUI under Level 4 information that is export controlled and "[o]ther information requiring explicit CUI designation" (such as "For Official Use Only"). Level 5 information, also Controlled Unclassified Information, "accommodates CUI that requires a higher level of protection than afforded by Level 4." SRG, § 3.2.5, at p.19. The Network Penetration DFARS includes "controlled technical information" and "export controlled" information within the four CDI categories, but does not use the SRG nomenclature.

[28] *Id*., Table 2 (DoD FedRAMP+ Security Controls/Enhancements), at pp.34-36). These are additional controls beyond those FedRAMP requires for civilian agency information of equivalent information impact.

[29] *Id*., Section 2.6, at 12. A graphical depiction of the relationship between the information impact level and the nature of required SRG cloud security controls is at http://www.doncio.navy.mil/Download.aspx?AttachID=6393.

When federal agencies use cloud services to perform their missions, the security requirements are rigorous. FedRAMP has been operational since January 2012.[30] Key stakeholders include the FedRAMP Program Management Office (PMO) and Joint Authorization Board (JAB), third-party Assessment Organizations (3PAOs), and Federal Agencies.[31] However, in the view of many observers, the process to demonstrate required security and receive the necessary JAB PA or Agency Authority to Operate (ATO) has proven to be both expensive and slow.[32] And when DoD uses the cloud, DISA imposes additional requirements beyond FedRAMP. A FedRAMP JAB PA or Federal Agency ATO will be used by DISA and DoD Components[33] for a DoD Authority to Operate, but the DoD ATO focuses on *mission risk* while the FedRAMP PA focuses on risk of the Cloud Service Offering.[34] The DoD process adds time and the SRG requires additional controls beyond FedRAMP counterparts for any information with impact above "Level 2" ("publicly releasable data"). Both FedRAMP and SRG invoke hundreds of controls and enhancements, drawn from NIST SP 800-53. In contrast to the high-level objectives set for industry by SP 800-171, the controls when cloud is used for federal information system purposes are highly-prescriptive and inflexible. This is not a workable – or necessary – approach to cloud security for commercial companies.

Cloud Security for "Covered Defense Information"

It is neither necessary nor prudent to require use of the FedRAMP process or for DISA to impose SRG "FedRAMP+" cloud security controls on the use by defense contractors of *Security as a Service* cloud offerings from third-party CSPs to protect CDI.

- **There is no legal requirement to limit CSPs for *Security as a Service* to those who have satisfied FedRAMP and obtained a FedRAMP JAB PA or an Agency ATO.** FedRAMP was established to enable agencies to satisfy FISMA.[35] FISMA applies only to federal agencies and to contractors who operate information systems, including cloud-based systems, "by … or on behalf of" the federal government.[36] In other words, FISMA and its "progeny" (such as FIPS 199 and FIPS 200, and SP 800-53) govern actions that federal agencies take to protect information in their possession and to safeguard information systems (including cloud) that they operate or that contractors operate on their behalf. These obligations do not extend outside the FISMA "envelope" to contractors who are provided, create, or use CDI (or other CUI) to deliver a product to, or perform a service for, the federal government.

---

[30] *See* "Federal Risk and Authorization Management Program (FedRAMP) – Agency Day," Jan. 20, 2012, *available at* http://www.gsa.gov/graphics/staffoffices/FedRAMP_1-20-12_Agency_Day_FINAL.pdf.

[31] FedRAMP Guide, at 13. The PMO and JAB establish processes and standards for security authorization. The 3PAOs are independent cloud "auditors," who perform initial and periodic assessment of FedRAMP controls that are implemented by CSPs. Federal agencies contract with CSPs and provide authorization to operate (ATO) when they have approved a cloud service for use by their agency. *Id*.

[32] E.g., "FedRAMP Process Takes the Heat on Capitol Hill," *MeriTalk*, Mar. 3, 2016, *available at* https://www.meritalk.com/articles/fedramp-process-takes-the-heat-on-the-hill/.

[33] A "DoD component" is defined as "a Military Department, Defense Agency, DoD Field Activity, or organization within the Office of the Secretary of Defense that provides or administers an award to a recipient. 32 CFR § 34.2.

[34] DISA, "Risk Assessment of Cloud Service Offerings," Apr. 22, 2016, at 6, *available at* http://www.disa.mil/~/media/Files/DISA/News/Conference/2016/AFCEA-Symposium/5-Bass_Risk_Assessment_Cloud.pdf

[35] *See* FedRAMP Guide, at 2, 9.

[36] FISMA requires agencies to provide information security "commensurate with the risk and the magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of (i) information collected by or on behalf of an agency; or (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency" (44 U.S.C. §3544(a)(1(A)).

- **The security methods of federal agencies are derived from FISMA and other statutes. Private organizations are not subject to the same obligations. Federal policy should recognize the converged security objectives of the public and private sectors, but not mandate federal-specific methods.** Federal agencies today perform their duties using a variety of systems. Legacy systems may be isolated and hard to support.[37] Federal policy recognizes that the cloud offers reduced capital and recurring costs and potential improvements to scale, functionality, and serviceability. However, agencies perceive risk in the "loss of control" that accompanies transition to the cloud. Many aspects of FedRAMP and the SRG can be understood as measures to mitigate risks perceived in loss of control.[38] Different concerns are present when the federal government contracts with private companies. In the contract relationship, agencies rely upon and share information with external (nonfederal) parties. The rules can and should differ between the acts of federal agencies in sovereign and ministerial functions, and the acts of agencies when purchasing from the private sector. In its business dealings with contractors, the government can, and should, accept security measures that are generated by, and used in, commercial markets. These serve purposes similar to FISMA, FIPS, FedRAMP, and so forth – but use different processes and allow different methods to achieve the objective of continuing security.

- **In SP 800-171, NIST lists controls to protect CUI in *contractor* information systems, which differ in number, nature, detail, and purpose from the SP 800-53 controls that apply to *federal* information systems. The same principle should be applied to cloud services used by federal contractors.** FISMA causes the federal government to consider security from the standpoint of information "confidentiality," "integrity," and "availability."[39] Federal Information Processing Standards (FIPS) 199 proscribes the method to categorize expected "impact" of loss in each of these three categories. FIPS 200 articulates the 17 "families" that organize the hundreds of detailed controls and enhancements collected in SP 800-53r4. SP 800-171 has a similar purpose, but different application. It uses 14 of the 17 control families of FIPS 200 and derives certain requirements from SP 800-53, but it states performance objectives without requiring the mechanics of SP 800-53r4.[40] Explicitly, the focus of SP 800-171 is on "protecting the *confidentiality* of Controlled Unclassified Information (CUI) in *nonfederal* information systems and organizations."[41] In contrast, many controls required by FedRAMP and by DISA through the SRG concern "integrity" and "availability," which are subordinate in SP 800-171. SP 800-171 treats all CUI in the hands of contractors as having "moderate" impact, without distinction.[42] Controls from FedRAMP or the SRG concerning "high" impact information are inappropriate and unneeded.

---

[37] E.g., "Federal CIOs need help with legacy-to-cloud transition," *CIO* website, Jun. 2, 2016, *available at* http://www.cio.com/article/3078555/cloud-computing/federal-cios-need-help-with-legacy-to-cloud-transition.html.
[38] E.g., Kirk Kern, "4 obstacles to federal cloud adoption," *Federal Times*, Jan. 5, 2015, *available at* http://www.federaltimes.com/story/government/solutions-ideas/2015/01/05/cloud-adoption-federal-meritalk/21296371/.
[39] 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, "Standards for Security Categorization of Federal Information and Information Systems," Feb. 2004, was developed by NIST to implement the three security objectives of FISMA – confidentiality, integrity and availability (FIPS 199, at 2).
[40] NIST SP 800-171, Ch. 1 at 6. SP 800-171 includes "mapping tables" that show which CUI security requirements correspond to SP 800-53 and to ISO/IEC 27001.
[41] *Id*., "Cautionary Note," at v.
[42] *Id*., Ch. 2, at 5.

- **To safeguard CDI in the cloud, DoD should accept a flexible, goal-oriented approach consistent with SP 800-171.** DoD's 2013 UCTI rule directed defense contractors to utilize a subset of fifty-one (51) controls taken from SP 800-53. However, in the 2015 CDI rule, DoD replaced SP 800-53 with safeguards reflecting SP 800-171, developed for commercial information systems. In the UCTI rule, DoD was content with only a small subset of the controls then available from SP 800-53. In the later CDI rule, DoD requires no controls directly from SP 800-53. The same approach should be taken when contractors use the cloud. When CDI is secured in the cloud, the level and nature of safeguards should be proportionate to what DoD has accepted as sufficient for "on-premises" systems, and not reflect the complexities and mechanics of SP 800-53 or the SRG.

- **A regime that enables contractors to use commercial CSOs for CDI (and CUI) should seek to "harmonize" the availability of other, commercial security regimes, and to exploit accreditations or certifications as may be achieved under those non-federal systems.** The NIST *Framework for Improving Critical Infrastructure Cybersecurity*[43] has been widely praised in the U.S. and abroad for the process of security assessment and control selection that it offers to diverse industries. The NIST Framework does not require use of any SP 800-53 controls. While it offers "informative references" to SP 800-53, these are listed along with other sources (e.g., COBIT, ISA or ISO/IEC) that can be consulted to achieve the purposes of the NIST *Framework*. Similarly, the Network Penetration DFARS invokes SP 800-171, but SP 800-171 requires *no* control or enhancement specifically as stated in SP 800-53r4.[44] For consistency, CSPs that offer *Security as a Service* should be able to consult and utilize SP 800-53 controls, as they consider helpful, without being required to do so.

Standards for Security as a Service: Relevance of FedRAMP and the SRG

Through the Network Penetration DFARS and SP 800-171, the precedent already is set for DoD to allow contractors to implement security measures for their "on-premises" systems, by reference to standards other than those NIST has developed for federal information systems. This leaves open the question of whether, and to what extent, FedRAMP or SRG processes and controls should apply when contractors place CDI (or CUI) in the cloud.

FedRAMP has been slow to authorize CSPs and many federal agencies have been slow to leverage ATOs where granted by different agencies. Nonetheless, there are signs that FedRAMP has expedited its process and the number of providers granted JAB PA or Agency ATOs has increased. As of the date of this writing, FedRAMP has identified four (4) cloud systems that have received JAB PAs as compliant with the new "High" impact security level and 17 that are compliant at the "Moderate" impact level.[45] 44 cloud systems have received agency authorizations.[46] More providers have started the process for a JAB Provisional Authorization or Agency Authority to Operate.[47] Through the "FedRAMP FASTForward"

[43] First produced in February 2014, the NIST Framework is *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[44] While SP 800-171 offers "maps" from its controls to SP 800-53 and to ISO/IEC 27001, these are non-exclusive.
[45] Webpage, "FedRAMP Compliant Systems," accessed Jul. 22, 2016, *available at* https://www.fedramp.gov/marketplace/compliant-systems/.
[46] *Id*.
[47] Webpage, "FedRAMP In-Process Systems," accessed Jul. 22, 2016, *available at* https://www.fedramp.gov/marketplace/in-process-systems/.

initiative, the industry has been working to improve and accelerate the FedRAMP process.[48] These accomplishments, and the industry's efforts, reflect both investment and accomplishment through FedRAMP, and suggest improvement ahead that will help achieve more adoption of cloud services by federal agencies for federal information systems.

There is value in any FedRAMP authorization and, as to DoD information, value where DISA has granted cloud authorization pursuant to the SRG. But the objectives of FedRAMP and the SRG differ from those of the Network Penetration DFARS (for CDI) and the future, similarly purposed, general Federal Acquisition Regulation (FAR) rules (for CUI). FedRAMP and the SRG rely upon a federally-defined and managed process, employing federally-specified controls, and subject to federally-directed authorization and oversight. Protection of CDI (and CUI) in contractor information systems may benefit from, but does not demand, identical process or security controls:

- **A CSP that has obtained FedRAMP or DoD authorization at the "Moderate" impact level or above should be deemed qualified to offer *Security as a Service* for the storage, processing, or transmittal of CDI (and CUI).**

- **FedRAMP or DoD authorization should not be *required* for *Security as a Service*.**

In the private sector, CSPs routinely handle massive quantities of information of great sensitivity. Many information types are stored or processed using the cloud, including Personally Identifiable Information (PII), Payment Card Information (PCI), Federal Tax Information (FTI), financial industry messaging, enterprise resource planning (ERP), human capital management (HCM), financial accounting, payroll, product lifecycle management (PLM), and law enforcement records – among others. Businesses worldwide depend upon the cloud for these functions. For customers and cloud service providers, sustained information security is a paramount objective. To thousands of commercial businesses, protection of information they entrust to public cloud security is just as important as federal interests in maintaining the "confidentiality" of CUI.

As noted earlier, DoD estimates that the Network Penetration DFARS may apply to 10,000 contractors, many of them small businesses. The National Archives and Records Administration (NARA) estimates that CUI is accessed by 300,000 entities.[49] Effective protection of massive amounts of CDI (and CUI) by so many diverse enterprises requires strategies, solutions, and providers outside the process constraints and exclusive control measures of FedRAMP or the SRG. *Security as a Service* should not be limited to providers with a FedRAMP JAB Provisional Authorization or Agency ATO. Contractors and other enterprises entrusted with CDI and CUI should be able to choose among many capable and trustworthy CSPs competing in a market for protection of public information in private hands.

Clarifications and Changes to the Network Penetration DFARS

DoD should clarify the DFARS and revise the FAQs and PGI, as necessary, to facilitate use of *Security as a Service*. It is necessary to confirm that, for the purpose of protection of CDI, contractors can use cloud services other than those that have FedRAMP or DoD SRG authorization. The Network Penetration DFARS was not written to accommodate use of third-party public cloud for CDI security. Unfortunately,

[48] *See* webpage, "FedRAMP FASTForward," *available at* http://www.fedrampfastforward.org/.
[49] "NARA preps for new info control rules," *Federal Computer Week*, May 28, 2016, *available at* https://fcw.com/articles/2015/05/28/nara-preps-for-rules.aspx.

as written, it can be understood to impose severe restrictions on cloud access for this purpose. Clarification is therefore necessary.

DFARS 239.7604(a) requires the use of DFARS 252.239-7009 ("Representation of Use of Cloud Computing") in solicitations "for information technology services." DFARS 239.7604(b) requires use of DFARS 252.239-7010 ("Cloud Computing Services") in solicitations and contracts "for information technology services." An initial problem is that "information technology services" contemplate the delivery of such services to DoD rather than (distinctly different) the *use* of an information technology *system* that is incidental to a contractor's delivery of a supply or service to DoD.

The Network Penetration DFARS includes the "Representation" (-7009) clause.[50] It is a "notice" clause that obligates an offeror to inform the government whether or not use of cloud computing services in the performance of any contract or subcontract is anticipated. DoD has issued Program Guidance and Instructions (PGI), which explain that the *only* cloud services that may be offered and approved are those that appear in the "DoD Cloud Service Catalogue." These must have DoD Provisional Authorization prior to award.[51] Consequently, it is conceivable that contracting officers may conclude, upon reading this language literally, that no contractor subject to the Network Penetration DFARS is permitted to use any cloud service that has not been approved by DISA in accordance with the SRG. This would be true even if the use of cloud was limited to security of CDI. Presumably, DoD did not intend that the "Representation" clause have this preclusive effect.

- DoD should clarify the DFARS, or the PGI, to inform DoD components and acquisition personnel that the "Representation" clause is not to be used *except* where DoD is purchasing "information technology services." It would not apply where an offeror or contractor elects to use commercial cloud service incidental to providing a service or delivering a product. This would avoid limiting contractor choice to the offerings in the Cloud Service Catalogue that have received DoD Provisional Authorization. DoD could require offerors and contractors to notify Contracting Officers when they intend to satisfy the Network Penetration DFARS through use of a cloud service.

The "Cloud Computing Services" clause (-7010) is expressly applicable "when using cloud computing *to provide information technology services* in the performance of the contract."[52] By its "plain words," the -7010 clause should control where DoD contracts with a company to provide or perform functions of a "federal information system." This clause also limits cloud services to those that satisfy the SRG. Because the -7010 clause is included with the Network Penetration rules, which otherwise focus on protection of CDI in *contractor* information systems, the risk of confusion is again present.

- Initially, DoD should explain in PGI for the Network Penetration DFARS, or by revision to the existing FAQs, that the "Cloud Computing Services" clause is intended for use only when DoD is purchasing services for "federal information system" purposes.

[50] 80 Fed. Reg. 51747 (Aug. 26, 2015).
[51] The same requirement applies where a contractor informs the contracting officer, after award, requesting the use of cloud services. *See* PGI 239.7603-1(a), (b), *available at* http://www.acq.osd.mil/dpap/dars/pgi/pgi_htm/current/PGI239_76.htm#239.7603.
[52] DFARS 252.239-7010(b) (emphasis added).

Beyond clarification, DoD should state any additional measures it expects when a contractor elects to secure CDI in the cloud. Study will be required to determine where additional measures are necessary and how to ascribe these to embrace leading commercial cloud service models and security methods. Initially, DoD may determine to require notification to the contracting officer, and/or to the DoD CIO office, when a contractor determines to satisfy the Network Penetration DFARS through a cloud service. DoD also may determine to include requirements in solicitations and contracts that set minimum service and security standards and reporting obligations when its suppliers contract for *Security as a Service*. (Federal civilian agencies can follow suit when the general CUI safeguarding rule is in place.) For such purposes, DoD should consider revision to the -7010 clause. Topics might include, for example:

- Reference to cloud-specific controls (a "cloud overlay" to NIST SP 800-171, if prepared) for commercial, public cloud used for information security
- Recognized industry standards and practices
- Accepted sources of third-party assessment and assurance
- Expected documentation of security practices and plans
- Government access rights to physical cloud infrastructure
- Necessary interface and connectivity protections
- Required encryption, access control, identity and access management
- Utilization of information rights management
- Continuous monitoring and event detection
- Required cloud service contract terms and conditions and SLA terms
- Additional cyber event reporting and response obligations
- Access to data and cooperation for forensic and remedial measures

Any required terms should principally serve the primary federal interest in assuring the *confidentiality* of CDI (and CUI). As to data *integrity* and *availability*, primary reliance should be upon the commercial service and SLA terms in agreements between contractors and cloud service providers. The Network Penetration DFARS relies upon NIST for safeguards to improve "on-premises" IT systems. A DFARS that accommodates cloud-based security should look to NIST as well, but not to the exclusion of other established, sufficient regimes. Regulations to protect CDI and CUI should not mandate the federal authorization process or impose federal-centric cloud security standards on the commercial cloud services available to federal contractors for security solutions.[53] Among defense and civilian agencies, a consistent approach should be pursued for strategy, review or authorization process, control methods, and for reporting and oversight.

Benefits of the Commercial Cloud Service Agreement and the SLA

Contractors who utilize *Security as a Service* will enter into Cloud Service Agreements (CSAs), as well as the Service Level Agreements (SLAs), with the Cloud Service Provider.[54] These contractual instruments define and assign rights and duties between the customer and the provider. Certain features impact the security of federal information when placed in a public cloud. Industry standards and best practices

[53] DoD already has decided that its contractors have until Dec. 31, 2017 to fully comply with NIST SP 800-171 for the protection of CDI for "on-premises" information systems. DoD must refrain from imposing DISA and the SRG requirements where a contractor subject to the Network Penetration DFARS decides to move CDI to the cloud.
[54] When it clarifies the Network Penetration DFARS to encourage *Security as a Service*, DoD could advise contractors that it has a right to require delivery of CSAs and SLAs should the government have cause to review cloud security measures. If experience indicates a need, the government could require delivery of CSAs and SLAs as part of the DFARS compliance obligation.

already address many key issues of federal concern. These need to be recognized – and encouraged – in any future federal rulemaking that affects use of public cloud to secure federal information. ISO 27017, for example, includes relevant recommendations for the Cloud Service Customer Agreement, such as allocation of basic roles and responsibilities between customer and provider (15.1.2); identification of applicable laws, regulations, and other requirements (18.1.1); and independent review of information security controls and guidelines (18.2.1).

In the DFARS (and later FAR) clauses that apply to contractor use of *Security as a Service*, the federal government should refrain from demands for special requirements unique to the use of cloud services by government contractors. The federal strategy should be to encourage and enable adoption of cloud for security solutions by all government contractors. Special federal demands for CSA and SLA terms will tend to work against adoption by government contractors because material distinctions in the terms of service could limit the cloud offerings available to government contractors. Much of cloud value is a function of both scale and consistency of implementation for all "tenants." Accordingly, restraint should characterize federal "intervention."

At the same time, federal agencies are subject to statute, regulation, and government-wide policies in their treatment of CDI (and CUI). When legally necessary, DoD and the civilian agencies can require special terms of service between government contractors and cloud service providers. NIST can assist by stating cloud-specific security objectives to address necessary federal interests.[55]

An "Overlay" to NIST SP 800-171

In SP 800-53r4, NIST has produced a "catalogue" of security controls and enhancements for federal information systems and for cloud operated by, or on behalf of, the federal government. These measures differ greatly in number and nature from the high-level controls that SP 800-171 provides for "on-premises" systems. For security of CDI (and CUI) from commercial cloud service providers, SP 800-53 should not be the baseline or otherwise required. For protection of CDI (and CUI) in the cloud, NIST should rely upon commercial process and methods, rather than the SP 800-53 regime developed for federal information systems. NIST can "map" to several sources of established commercial cloud security standards and practices.

- ISO/IEC 27017, "Information technology – Security Techniques – Code of Practice for information security controls based on ISO/IEC 27002 for cloud services"[56]
- Cloud Security Alliance (CSA), Cloud Controls Matrix (CCM),[57] and Security Trust & Assurance Registry (STAR)[58]
- SANS Institute, Implementing the Critical Security Controls in the Cloud, and Cloud Security Framework Audit Methods[59]

[55] By using a "goal" approach, like that already employed by SP 800-171, the federal government can encourage contractors who choose cloud to achieve general objectives without dictating how these are to be met.
[56] Accessed on Jul. 26, 2016, *available at* https://www.iso.org/obp/ui/#iso:std:iso-iec:27017:ed-1:v1:en.
[57] Cloud Controls Matrix v.3.0.1, Jun. 6, 2016 update, *available at* https://downloads.cloudsecurityalliance.org/assets/research/cloud-controls-matrix/CSA_CCM_v.3.0.1-06-06-2016.xlsx.
[58] Accessed on Jul. 26, 2016, *available at* https://cloudsecurityalliance.org/star/.
[59] Accessed on Jul. 26, 2016, *available at* SANS Institute, Reading Room, https://www.sans.org/reading-room/whitepapers/cloud.

- Center for Internet Security, Critical Security Controls (applied to the Cloud)[60]

Several of these involve third-party accreditation and certification, as well as other forms of disclosure and review that add confidence to those who rely upon the security of cloud services. Commercial cloud service providers perform business functions for tens of thousands of customers who entrust to these CSPs millions of records that are subject to law, regulation, or other security or privacy obligation, as well as vast amounts of technical data and proprietary information. For much of this information, the source of privacy and security requirements are the same "laws, regulations, and Government-wide policies" that cause the National Archives and Records Administration (NARA) to categorize information as one or another form of CUI.[61] This "commonality" between legal obligations to protect certain information types in private sector commerce, and federal obligations to protect CUI, should encourage reliance upon proven commercial security methods, such as those that CSPs regularly and successfully employ to serve a multitude of industry sectors and purposes.

Recent years have exhibited an "explosion" in the rate and scale of adoption of cloud services and in the use of cloud for enterprise-critical functions. In fact, market acceptance of cloud would not have been accomplished without the continuous delivery of "adequate security" in a dynamic threat environment.[62] Rather than elaborate exercises in documentation, federal agencies should seek a record of achieved security when they entrust CDI (or CUI) to contractors or other nonfederal enterprises. DoD, NIST, and other involved federal agencies should exploit, not deny, the security capabilities of commercial cloud service providers. A cloud "overlay," if produced for SP 800-171, should avoid federal-unique requirements and add requirements only as necessary to protect important federal interests. The "overlay" should encourage, not frustrate, cloud access.

Superior Results through *Security as a Service*

Readily Employable by Diverse Defense Contractors

The difficulty of achieving compliance with SP 800-171 varies enormously with the nature of the company's business, the information it hosts and uses, and the preexisting information systems and controls. Some companies approach the problem by trying to elevate their security to SP 800-171 requirements at the enterprise or domain level for all IT systems. Other companies seek to identify CDI within an enterprise and then isolate this information into separate information systems or logical domains. Planning execution of even these preliminary steps can be very time-consuming, resource-intensive, and expensive. Actual implementation of required controls or improvements adds to the time needed, the administrative and resource challenges, and the costs.

---

[60] *See* Bart Westerlink, "Applying the CIS Critical Security Controls to the Cloud," Apr. 26, 2016, *available at* http://www.isaca.org/chapters7/Sacramento/Events/Documents/PResentation_20160426_Top20Secuirty%20Controls%20to%20the%20Cloud.pptx.

[61] Proposed CUI Rule, § 2002.11(a) ("CUI categories and subcategories"), 80 Fed. Reg. 26506 (May 8, 2015).

[62] A subject worthy of study, but beyond this paper, is the comparative cybersecurity record of cloud versus "on-premises" information systems in recent years. Many of the most-publicized attacks (e.g., Sony, Target, Office of Personnel Management, appear to have been made against "on-premises" systems). Some articles assert that there have been fewer breaches of cloud systems. *See, e.g.,* Business Insurance, "Cloud computing data breaches currently few," accessed on Jul. 26, 2016, *available at* http://www.businessinsurance.com/article/99999999/NEWS070101/399999805.

In contrast, *Security as a Service* is a very attractive alternative; one that many companies can accomplish more quickly, with less need for expert resources, and at lower cost. Once identified, CDI can be entrusted to a CSP who is contractually obligated to meet and sustain compliant protections. The DFARS (or FAR) contractor compliance obligation is satisfied through reliance upon the *Security as a Service* provider for the CDI (or CUI) in the cloud. This choice lets companies continue to use other security practices for the remainder of their enterprise. Like other forms of cloud services, *Security as a Service* will be demand-based and scalable, leveraging resources and expertise for multiple information tenants and security clients.

Greater Investment by CSPs

DoD's approach to CDI and the SP 800-171 safeguards rely upon contractors' self-assessment (against SP 800-171) without an authorization or accreditation mechanism.[63] Monitoring is expected "on an ongoing basis," but not continually (SP 800-171 at 3.12.13). This places a great deal of trust in the assertions of each contractor that is, or will become, subject to SP 800-171.

By comparison, DoD can have much higher assurance in actual (versus "promised") security from CSPs who offer *Security as a Service*. Because the commercial business of CSPs depends upon effective security delivered over time, market forces will motivate diligence, responsiveness, and continuing updates to threat assessment, vulnerability detection, and protective measures. CSPs are likely to obtain private insurance that will be accompanied by its own due diligence (risk review) process. As a matter of investment, CSPs – serving many customers via typical models of public, community, or hybrid cloud – spend vastly more on continuing security updates than can be expected from all but a few of the thousands of companies in the defense supply chain. CSPs already demonstrate their security by reference to a number of international regimes, such as ISO, the Cloud Security Alliance (CSA), and American Institute of Certified Public Accountants/Service Organization Control (AICPA/SOC) Reports. These organizations encompass technical specialists, standards-setting bodies, and methods for assurance, accreditation, and certification. The federal government will benefit by enabling recipients of CDI (and CUI) to use CSPs whose security is subject to these assurance programs. CSPs that have adopted these standards or earned their accreditation will be better informed about persistent, adaptive, and continuous threats, faster to find and implement advanced detection and protection measures, and better prepared to promptly respond to attacks and recover quickly.

Information Rights Management

The approach of NIST SP 800-171 focuses upon protection of "on-premises" information systems as the means to protect the information hosted on those systems. We might take a lesson from several of the notorious security breaches of recent years. Protection of the information system, as if it were a "citadel" or a "castle" protected by external barriers (e.g., firewalls) constituting a veritable "moat," has not worked well where massive amounts of data, once extracted from the system, become unprotected and freely transferable. Technical measures are available to encrypt, and otherwise control, even deny, access and use rights. IRM provides a means to retain control over sensitive information – such as CDI and CUI – and to extend that control "beyond the perimeter" and subsequent to a breach. With IRM,

[63] *Compare* DoD security practices as expressed in DoD Instruction (DoDI) 8510.01 – the "Risk Management Framework" (or RMF). Department of Defense Instruction (DODI) 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," Mar. 12, 2014, Incorporating Change 1, Effective May 24, 2016, *available at* http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf. The RMF describes six security steps: (1) Categorize System, (2) Select Security Controls, (3) Implement Security Controls, (4) Assess Security Controls, (5) Authorize System, and (6) Monitor Security Controls. *Id*., at 28.

these capabilities are persistent, remaining in place even after initial transfer to an intended and authorized recipient, where access and use privileges subsequently change, and even in the event of a successful but unauthorized extraction.

Information rights management is especially valuable if we discriminate among the four existing types of CDI and what is expected among the many categories and subcategories of CUI. Many types of information are subject to multiple legal or regulatory sources of controls. (Examples include export controlled information, law enforcement information, HIPAA or PII, payment card information, and the like.) Controls that focus upon the information system tend to apply a common set of protective measures to all of the information in that system. An information rights management system can discriminate in the selection and application of controls at the document or file level. There are attractive synergies that accompany the use of information rights management for supply chain coordination. Under the Network Penetration DFARS, higher tier contractors are responsible for the cybersecurity measures of their lower tier sources. Many higher tier contractors also have the obligation to manage access to information among a diverse and sometimes international supply chain where export controls apply in a non-uniform fashion to some data and to some recipients. Building IRM into a cloud-based supply chain management system can provide high levels of access control, enhance export compliance, and protect both customer and contractor data even after an information system security breach. IRM systems can be accompanied by sophisticated data collection and analytic tools, which can reduce exposure by detection of unusual usage and trigger alerts where patterns of information access or utilization violate established norms.

Multifactor authentication (MFA), an example of IAM, is among the most important of the security controls emphasized by DoD, other federal agencies, and NIST. Advanced methods of IAM and IRM, when combined, control not only the key question of which individuals receive authorization to enter a network (and for what purpose), but what information each individual may access (and what privileges or limitations attach). Policy-based IRM systems can be implemented with MFA in ways that are largely transparent to the individual user but which provide defense in "breadth," "depth," and "duration" against unauthorized access or misuse.[64] Federal cyber initiatives should enable these technologies, which may be optimally employed in multi-tenant cloud platforms.

[64] The NIST Framework Core provides five categories of key cybersecurity outcomes: Identify, Protect, Detect, Respond, and Recover. *Framework for Improving Critical Infrastructure Cybersecurity*, *supra* n.42. Advanced IAM and IRM improve outcomes for event detection, incident response and system recovery, when compared to security strategies that rely upon peripheral defenses.

Conclusion

Cloud-based *Security as a Service* potentially answers the implementation challenge faced by thousands of companies in the DoD supply chain as they seek to comply with the Network Penetration DFARS. DoD suppliers should have the option of entrusting CDI to CSPs, essentially relying upon that provider to deliver the safeguards required by the DFARS and SP 800-171. *Security as a Service*, as a business proposition, is an attractive alternative to investments in "on-premises" information systems and increased recurring expense to maintain controls just to satisfy the demands of DoD customers. Companies should know they can move their CDI to secure cloud environments and still have access to the information they need to perform their DoD contracts – without an obligation to make the entirety of their information system(s) conform to the DoD-specific rules. For this to be achieved, DoD and NIST must identify and address issues that concern cloud-based *Security as a Service*. Clarification of the DFARS and its implementation guidance will be needed. NIST and DoD should coordinate with industry resources to determine whether to add a cloud "overlay" to SP 800-171. The imposition of federal-unique requirements should be carefully limited to encourage competitive, commercial CSPs to offer affordable, successful security solutions. These actions should be taken now and then refined in the general federal FAR regulations that will require security protection for all CUI.

---

[*] Robert S. Metzger is a partner of Rogers Joseph O'Donnell, PC, and head of the firm's Washington office. Mr. Metzger was named a 2016 "Federal 100" awardee by *Federal Computer Week*, which said of him: "In 2015, he was at the forefront of the convergence of the supply chain and cybersecurity, and his work continues to influence the strategies of federal entities and companies alike." Mr. Metzger is a member of the Defense Science Board Cyber/Supply Chain Task Force. He also is Vice-Chair of the Cyber/Supply Chain Assurance Committee of the IT Alliance for Public Sector (ITAPS), a unit of the Information Technology Industry Council (ITIC), a prominent trade association. **This paper 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.**