Bloomberg Law

Federal Contracts Report™

Cybersecurity

Regulations and contract requirements are imperfect but necessary means to achieve cybersecurity goals. Those responsible for the regulations, standards and contractual implementation must consider whether their actions are proving effective and if the results justify the costs.

Cyber Protection of CDI: Changed Requirements, New Methods, More Questions

BY ROBERT S. METZGER

The Defense Department (DOD) is using its acquisition authority to require all of its suppliers to improve their cyber protection of information and information systems. On Oct. 21, 2016, DOD revised and finalized its rule, ''Network Penetration Reporting and Contracting For Cloud Services.'' 81 Fed. Reg. 72986. 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.

Significant changes were made in the Defense Federal Acquisition Regulation Supplement (DFARS) final rule. DOD also has made available frequently asked questions (FAQs) that address many issues of application or interpretation. This article considers five key areas that concern industry: designation, scope, methods, adoption and compliance.

Robert S. Metzger, rmetzger@rjo.com, heads the Washington office of Rogers Joseph O'Donnell, PC, a boutique law firm specializing in public contracts. A frequent contributor to Federal Contracts Report, 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.

Designation: Who Determines What Is 'Covered Defense Information'?

The principal problem is that companies read the DFARS as requiring them to identify and protect all forms of controlled unclassified information (CUI) even though it may have come from federal agencies without designation or marking. The DOD may intend to limit the DFARS to information that it provided to its contractors, but, as explained below, ambiguities in the crucial language defining covered defense information

(CDI) expose contractors to doubt as to how much they protect or who is responsible to designate CDI.

CDI now includes unclassified controlled technical information (CTI), with military or space significance, ''or other information as described in the [National Archives and Records Administration] CUI Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies.'' DFARS 252.204-7012(a) (Definitions). The expanded definition of CDI, to include *all* of the CUI forms, creates uncertainty and will require additional and potentially unintended work unless clarified. Companies must locate and identify the other forms of CUI. Civilian agencies may not have ''designated'' or marked such information; indeed, the origin of such information may be unknown, even if the information type falls within a CUI category or subcategory. Companies then must assess the present methods they apply to secure various types of CUI, to determine whether protections meet the requirements of NIST Special Publication (SP) 800-171. 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.

DOD's position means that defense contractors must protect not only information of military or space significance, and that of ''operationally critical support,'' but also all of the other categories and subcategories of CUI that any element of their enterprise may use or possess. This is true even though civilian agencies have not yet implemented the ''agreement'' requirements that would impose SP 800-171 on any of the various ''nonexecutive branch'' entities who are afforded access to the CUI of these agencies.

Key to the ''designation'' problem is whether contractors must protect information already in their possession, before they take a contract subject to the -7012 DFARS, or only CDI received subsequent to such contracts. DOD could answer the concerns of many contractors simply by clarification that the DFARS do not apply retroactively and that a contractor has no duty to ''look back'' to determine whether information already in its possession is a form of CUI that requires protection.

Even though CUI categories other than CTI merit protection, DOD can decide to give priority to the protection of CTI — that of military and space significance. Protection of CDI requires action by DOD components to designate and mark information. Because some requiring activities may experience difficulty in satisfying these obligations, DOD should consider phased implementation as to CDI categories other than CTI. Many of the ''other'' CUI categories that concern *individuals*, such as personally identifiable information (PII) and protected health information (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 would 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 and produce better security sooner for CTI.

Scope: Does CDI Include 'Nonfederal' Information?

The revised DFARS definition, unfortunately, creates uncertainty as to what information is CDI and 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 information that is marked or otherwise identified in the contract, as well as 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.'' DFARS 252.204-7012 (a).

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. CDI, according to the plain words of the DFARS, 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, CDI may include any form of 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:

■ If information that fits a CUI definition is hosted, processed or transmitted in a management information system (such as an earned value, estimating or property management system), and the contractor ''uses'' that information to manage contract performance, is that use ''in support of'' contract performance, such that the DFARS and SP 800-171 apply to these systems?

■ 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 are also ''in support of'' contract performance?

■ Contractors frequently develop ''background'' intellectual property (IP), at private expense, which they use to furnish supplies to the government or perform a service. Such IP may be subject to International Traffic in Arms Regulations (ITAR) controls, if it has military application, or Export Administration Regulations (EAR) controls, if it is dual-use. Export-controlled information is one CUI category. This raises the question of whether the regulations apply to all export-controlled information — ITAR or EAR — that contractors use, possess or transmit. If the contractor uses such IP only to provide a supply or perform a service, but did not receive the IP from the government, does not furnish the IP to the government and does not export the IP, is it nonetheless subject to the DFARS and SP 800-171?

■ The revised DFARS definition, unfortunately, creates uncertainty as to ''what'' information is CDI and 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.

  FCR ISSN 0014-9063

DOD should clarify the definition of CDI to include *only* CUI that *DOD* furnished its contractors on contracts that incorporate the -7012 clause, *and that DOD designated* as CUI subject to protection. The ''in support of'' language invites misinterpretation and confusion.

Methods: What Is a Permissible Use of Cloud Services?

The focus of the DFARS and SP 800-171 are on the information systems owned and operated by contractors, i.e., ''on-premises'' systems. In the commercial world, the paradigm is shifting from ''on-premises'' information technology to the cloud. Until the October 2016 revisions, the DFARS did not address use by DOD contractors of external cloud services. Now, the ''safeguarding'' clause authorizes a contractor to use ''an external cloud service provider'' that meets security requirements ''*equivalent to* those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.'' DFARS 252.204-7012(b)(2)(ii)(D) (emphasis added).

It is positive that DOD now accepts use of FedRAMP-authorized cloud. But the ''window'' is not open enough. 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 uses federal-specific cyber controls and enhancements. (FedRAMP ''Moderate'' invokes 326 security controls derived from Special Publication 800-53, which the National Institute of Standards and Technology has prepared for use by federal agencies to assess and implement security and privacy controls.) Many world-class cloud service providers (CSPs) achieve security equal to or better than that of FedRAMP Moderate without use of the FedRAMP process or NIST controls. A DOD contractor subject to the DFARS cannot use these CSPs to host, process or transmit CDI, unless the contractor can establish that the controls of the CSP are ''equivalent to'' FedRAMP Moderate.

DOD needs to accommodate cloud service providers who employ nonfederal security techniques. It needs to promptly determine what is meant by ''equivalent'' to FedRAMP Moderate, who will decide, and which security measures (both for the CSP and the cloud service client) are sufficient. Among other questions to consider:

- Cloud is all but unmentioned in SP 800-171. NIST should prepare a ''cloud overlay'' to SP 800-171 that informs both contractors and CSPs of which security measures may be required when cloud is used as an extension of a contractor information system. NIST and DOD have identified cloud-specific security concerns, both for the provider and for the cloud customer. An overlay should identify key cloud-specific requirements, distinct from the existing 110 SP 800-171 safeguards. These requirements should be described functionally, as NIST has done throughout SP 800-171, drawing from the measures in SP 800-53 used for FedRAMP cloud security authorization. CSPs should be afforded flexibility to demonstrate their security methods, where based on accepted standards differing from FedRAMP, satisfy the security objectives of SP 800-171.

- DOD has a separate DFARS, 252.239-7010, for when cloud is used for an IT service or system operated ''on behalf of the Government.'' Should DOD create a ''dedicated'' clause when an ''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).

- Does the flowdown (DFARS 252.204-7012(m)) apply to enterprise agreements to use cloud services? Cloud-delivered functions that support business systems may routinely involve access to CUI. Is the cloud user responsible to assure compliance or compel incident reporting on the part of its CSP? Do such arrangements require the use of a cloud authorized at the FedRAMP Moderate level?

Adoption: How Can DOD and the DIB Assist Small Business?

The defense supply chain not only depends upon smaller businesses but increasingly seeks them out to leverage technology and agility. Concerns about the ability of small business to accommodate the ''network penetration'' DFARS and SP 800-171 are not new. But they have not been satisfactorily addressed.

- DOD should actively seek input from the small-business community, working with NIST, the Small Business Administration (SBA), and DOD's Office of Small Business Programs. Small businesses may not be heard from in Washington-area meetings with large contractors and prominent trade associations. Public meetings at diverse locations are advisable.

- Many small businesses are not well-informed of what DOD will permit in the achievement of DFARS compliance. Companies may satisfy the DFARS, even if not in full compliance with SP 800-171 by Dec. 31, 2017, if they have a sufficient system security plan, and intend to respond to gaps and mitigate vulnerabilities. It is especially important to inform small and medium-sized businesses how they can combine a system security plan (SSP) and action plan to get ''schedule relief.''

- DOD should prepare an implementation guide for small business and provide an accessible, automated self-assessment tool. DOD might adapt the Department of Homeland Security Cybersecurity Evaluation Tool (CSET) to help businesses assess their cybersecurity against different safeguarding regimes, including SP 800-171.

- DOD should consider creation of a ''facilitation'' resource specifically equipped and tasked to help with cyber compliance by small and innovative, nontraditional businesses. DOD could fund and cooperate with the SBA to establish a dedicated resource unit that would provide consultation and guidance to eligible companies.

- DOD should fund prime contractors to mentor, enable and otherwise assist downstream suppliers achieve the desired cybersecurity. Prime contractors have enormous leverage and contractual privity with their supply chain. 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 for Improving Critical Infrastructure Cybersecurity*. The Commission on Enhancing National Cybersecurity advocated greater use of the Framework in its

Dec. 1, 2016, ''*Report on Security and Growing the Digital Economy*.'' 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.''

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?

The ''compliance'' clause, required in all DOD solicitations, requires every offeror to ''represent'' that it ''*will* implement'' the security requirements of SP 800-171. DFARS 252.204-7008(c)(1)(emphasis added). The ''safeguarding'' clause, DFARS 252.204-7012(b), imposes on contractors an obligation to ''provide adequate security.'' A contractor's information system shall be subject to SP 800-171. As to oversight, DOD has explained: ''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 encourage third-party assessments. 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. FAQs, Q&A 25 (emphasis added).

This approach leaves companies unsure of what to do and whether they have done enough. Companies should expect scrutiny of their cyber safeguards after a breach. The DFARS requires rapid reporting of ''cyber incidents.'' DFARS 252.204-7012 (c). DOD has issued procedures, guidance and information (PGI) for the DFARS, which instruct DOD components what to do once a report is received. If requested by the requiring activity, the contracting officer shall ''request a description of the contractor's implementation'' of the SP 800-171 requirements ''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.'' PGI 204.7303-3(a)(3).

Nothing in the DFARS, or in the FAQs or PGI, informs contractors of the consequences of a finding of inadequate controls or deficient implementation. 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, and even exposure under the False Claims Act. Beyond this, companies have to consider the implications of noncompliance as to past performance reports, their eligibility for future contracts, or competitive position.

Any company may suffer a breach, irrespective of security measures. The report of a breach incident will prompt DOD to evaluate and perhaps investigate. Contractors have reason for concern about the business and liability risks, should DOD find their cyber safeguards inadequate. Companies striving for compliance need protection against these risks. As a matter of high priority, DOD should establish a ''*safe harbor*'' regime to reduce uncertainty and assure companies that they will be found in compliance:

- 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.

- A ''safe harbor'' (''acceptable'' compliance with the DFARS and SP 800-171) shall attach to a contractor's good faith implementation of an SSP and ''plan of action'' as submitted to DOD where DOD has not informed the contractor of objection or direction to take corrective or additional measures. The ''safe harbor'' should include contractors whose SSP and plan indicate that full compliance will not be achieved until a date subsequent to Dec. 31, 2017, provided that there is good-faith pursuit of the security objectives and implementation measures set forth in the plan.

- Higher-tier contractors cannot be guarantors of the cybersecurity of their supply chain, even though they have important responsibilities. 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; (iii) takes reasonable measures to assure lower-tier compliance. The determination of ''reasonable measures'' would be context-specific and risk-informed. Requiring activities could address specific requirements in solicitation documents. Reasonable measures could be requests for supplier representation of compliance, recognition of third-party assessments using accepted tools, and satisfaction of purchaser due diligence for cyber qualification.

Conclusion

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 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.

  FCR ISSN 0014-9063