Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity

The Department of Defense (DoD) published The ''Network Penetration'' Interim Rule. The community affected by the 'Network Penetration' DFARS is very large, and with all of the open implementation questions and areas of apparent conflict within the Rule at present, interested parties should consider making submissions, the author writes.

Government Operations

Twists and Turns—DoD Backs Away from the 'Network Penetration' DFARS. Or Does It?

BY ROBERT S. METZGER

On Aug. 26, 2015, the Department of Defense (DoD) published an Interim Rule, *Network Penetration Reporting and Contracting for Cloud Services*. The ''Network Penetration'' Interim Rule revised provisions of the Defense Federal Acquisition Supplement (DFARS) with the objective to protect four categories of ''Covered Defense Information'' (CDI) when used by contractors. It also invoked the new National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, ''Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,'' as the basis for required cyber controls.

Robert S. Metzger is a shareholder and heads the Washington, D.C. office of Rogers Joseph O'Donnell, PC (RJO). This article presents his individual views and should not be attributed to any client of RJO or to any organization with which Mr. Metzger is or may be affiliated.

On Dec. 29, 2015, Bloomberg BNA published my article, *Learning to Live with the 'Network Penetration' DFARS*, 104 FCR 1293, which examined six key implementation issues arising from the DFARS. Just a day after publication, on Dec. 30, 2015, DoD issued an Interim Rule revising the 'Network Penetration' DFARS.[1]

Changes to the Interim DFARS. Promulgation comments appearing in the Federal Register on Dec. 30, 2015, 80 Fed. Reg. 81472, seek to explain this second Interim Rule. The context was set on Dec. 14, 2015, when DoD held a public meeting to receive industry reaction to the Interim Rule. At that meeting, and elsewhere, DoD heard that many companies considered the 'Network Penetration' DFARS too demanding and sought more time for implementation.

In sum, the second Interim Rule accomplished the following:

- Offerors are provided additional time to be in compliance with NIST SP 800-171, which now must be in place no later than 12/31/2017;
- The DFARS clause was modified to require contractors to notify the DoD Chief Information Officer

[1] The link to this revision is at https://www.gpo.gov/fdsys/pkg/FR-2015-12-30/pdf/2015-32869.pdf.

 ISSN 1538-3423

(CIO) of any SP 800-171 security requirements that are not implemented at the time of contract award, within 30 days of contract award;

■ Subcontractor flowdown requirements were amended to require inclusion of the clause at DFARS 252.204-7012 (''Safeguarding Covered Defense Information and Cyber Incident Reporting'') (Dec. 2015) without alteration;

■ Amendments also limit the flowdown requirement only to subcontractors where their efforts will involve CDI or where they will provide ''operationally critical support;'' and

■ Where a contractor proposes ''alternative but equally acceptable security measures'' to those stated by SP 800-171, the requirement is removed that the contractor must receive approval from the DoD CIO prior to award.

As explained below, DoD's grant of temporal relief is accompanied by a new duty to notify the DoD CIO of unmet SP 800-171 requirements. This will cause thousands of companies potentially subject to the Rule to conduct a self-assessment of existing cyber practices. DoD explains that the additional implementation period will have a ''significant beneficial economic impact on a substantial number of small entities'' subject to the Rule. 80 Fed. Reg. 81473. But these companies are subject to full flowdown, without alteration, if their contract or purchase order involves any form of CDI. Beyond postponement of the full compliance ''due date,'' the second Interim Rule does little to respond to the challenge that the 'Network Penetration' DFARS poses to many companies.

Many Implementation Issues Remain Unresolved. My previous article examines six key implementation issues. The second Interim Rule (also referred to as the ''Dec. 30 revision'' and the ''revised Rule'')) answered some concerns there raised and touched upon others, but many were not addressed.

Did DoD Postpone Implementation of the DFARS?

The ''Compliance'' clause, at DFARS 252.204-7008(c)(1) (Dec. 2015), must be used ''in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items.'' DFARS 204.7304. This, the -7008 clause, now obligates contractors to represent that they will implement the security requirements ''not later than December 31, 2017.'' The ''Safeguarding'' clause, at DFARS 252.204-7012(b)(1)(ii)(A) (Dec. 2015), is to be used ''in all solicitations and contracts,'' also including FAR part 12 procedures. DFARS 204.7304. The -7012 clause states that contractors are to implement the security requirements of SP 800-171 ''*as soon as practical*, but not later than December 31, 2017.'' (Emphasis added.) Further, the ''Safeguarding'' contract clause adds an obligation that a contractor ''shall notify the DoD CIO . . . within 30 days of contract award, of *any* security requirements specified by NIST SP 800-171 not implemented at the time of contract award.'' DFARS 252.204-7012(b)(1)(ii)(A) (Dec. 2015) (emphasis added). The post-award duty to notify DoD of ''gaps'' against the NIST requirements is not limited to DoD primes.

Companies that already have completed a cybersecurity self-assessment may be able to meet the 30-day notification deadline. But many of the approximately 10,000 companies subject to the Rule likely confront the Network Penetration' DFARS without that foundation. An important feature of the revised Rule is that these companies are not forced either to ''opt out'' of a subject procurement or to assert immediate compliance when it has not been achieved. Rather, if a company is beginning to address cybersecurity mandates, it can respond to a solicitation and receive an award even if it has neither completed a self-assessment nor complied with a single NIST SP 800-171 requirement. In this situation, a company (or a subcontractor) can inform the DoD CIO that it does not meet any of the SP 800-171 requirements – and this notification is due only after award. DFARS 252.204-7012(b)(1)(ii)(A) (Dec. 2015). The company's obligation, in this scenario, is to satisfy NIST SP 800-171 safeguards ''as soon as practical, but not later than December 31, 2017.'' *Id*.

The language of the ''Safeguarding'' contract clause, at DFARS 252.204-7012(b)(1)(ii)(A) (Dec. 2015), contains potentially contradictory language. Is the phrase ''as soon as practical'' only precatory (a ''wish'' or ''request'') or is it obligatory? Who decides? Perhaps this phrase was intended to recognize companies who already have complied with the predecessor Rule, published in 2013, that concerned ''Unclassified Controlled Technical Information'' (UCTI).[2] Or, it may be to encourage those companies now working to comply with first 'Network Penetration' Interim Rule published in August, 2015. Contractors will need clarification. The new language will be read by some to postpone compliance for all companies for two years. This may not serve the national interest, at least as to companies in the defense supply chain who already satisfy the UCTI.[3] Conceivably, a Requiring Activity may determine that its work involves especially sensitive information and cause a given solicitation to require bidders to provide protection *before* the final ''due date.''

While full compliance with SP 800-171 is not required until the end of 2017, DFARS 252.204-7012(b) (Dec. 2015) requires contractors to provide ''adequate security'' for CDI – an obligation that arises immediately and is not deferred. Should a cyber event occur before Dec. 31, 2017, the Government could assert that earlier conformance with NIST SP 800-171 controls was ''practical'' for the affected contractor and that failure to protect affected information is a breach of the duty to provide ''adequate security.'' Companies cannot now be sure when they will be held obligated to comply. Prudent companies would be well-counseled not to wait to implement the required controls.

Who Is Responsible to Identify ''Covered Defense Information''?

An issue that has troubled industry is whether DoD will acknowledge it is obligated to inform its contractors when they are to host, transmit or use CDI that is subject to the 'Network Penetration' DFARS. The sec-

[2] *Safeguarding Unclassified Controlled Technical Information*, (DFARS Case 2011–D039), 78 Fed. Reg. 69273, Nov. 18, 2013, available at www.gpo.gov/fdsys/pkg/FR-2013-11-18/pdf/2013-27313.pdf.

[3] Many sources establish the genuine national interest in assuring the confidentiality of DoD's sensitive but unclassified information. A threat-driven or risk-based analysis may cause some DoD Requiring Activities to conclude that they cannot risk a two-year hiatus before ''their'' CDI will have assured protection. It will not be surprising to see cyber protection obligations that are both more urgent and more demanding imposed for some programs.

  PVLR ISSN 1538-3423

ond Interim Rule did not deal with this topic, although it is addressed in the ''Frequently Asked Questions'' (FAQs) and Procedures, Guidance and Information (PGI) for the 'Network Penetration' DFARS published by DoD on Nov. 17, 2015.[4]

A special problem is presented by export-controlled information – one of the four types of CDI that are made subject to cyber protection requirements by the 'Network Penetration' DFARS. There is both a national interest and a business interest (both proprietary and regulatory) in the protection of export-controlled information against unauthorized access. Companies who create or possess such information already are subject to obligations, under the relevant export control laws and regulations, to protect such information. However, many companies in the defense supply chain will author, revise or use information subject to export controls, in the performance of defense contracts, *but not* provide that information to their DoD or higher tier prime customer. The Nov. 2015 FAQs and PGI do not provide guidance on the subject of whether or on what basis DoD will identify export-controlled information subject to the Rule. DoD should limit the 'Network Penetration' Rule to *DoD* or other *government* information that it provides to its contractors or pays its contractors to develop and deliver to it. It should not impose contractual cybersecurity mandates on forms of *contractor* information and data that are not deliverable. To attempt to do so will be unworkable.

Many companies in the defense supply chain employ sensitive and proprietary information to make products or services that DoD needs, but DoD does not necessarily purchase the underlying technology or data. DoD's receipt of hardware, or benefit from the service, should not impose upon the supplier DoD-specific (even ''unique'') cyber protection obligations. The core purpose of the federal government's ''controlled unclassified information'' initiatives is to protect *federal* information when it is hosted or used by contractors or transits contractor systems. That is distinct and different from protection of *contractor* information used to provide a product or service; the presence of export controls imposes a regulatory obligation upon the contractor but does *not* cause such information to become ''federal'' information subject to federal cyber safeguarding mandates.[5]

How Does the DFARS Affect Smaller Businesses?

The ability of smaller companies to comply is a crucial obstacle to successful implementation. In the promulgation comments, DoD estimates that the 'Network Penetration' Rule may apply to 10,000 contractors of which ''less than half'' are small businesses. *Id*. If companies decline to participate in new procurements because they cannot comply with the DFARS, there is a potentially crippling effect upon DoD's acquisition system. The second Interim Rule acknowledges industry concerns about the challenge for small businesses and provides relief in 2-year postponement for full compliance with NIST SP 800-171 safeguards. The ''Safeguarding'' (-7012) contract clause, where if flows down to a small business, imposes immediate obligations to ''rapidly report'' cyber incidents to DoD. DFARS 252.204-7012(c)(Aug. 2015). Once a small business (or other supplier) accepts a contract subject to the -7012 clause, it is then subject to the reporting obligation, which is not postponed. The ability to report a cyber incident presupposes the existence of a cyber defense or monitoring capability that companies subject to this Rule may not possess at the time it first applies to them.

A lower tier supplier subject to the 'Network Penetration' DFARS must represent, when it submits an offer, that it ''will implement'' the security requirements of SP 800-171 ''not later than Dec. 31, 2017.'' DFARS 252.204-7008(c)(1) (Dec. 2015). Moreover, the revised Rule now requires flowdown of the ''Safeguarding'' (-7012) contract clause, ''without alteration, except to identify the parties,'' whereas before a contractor had only to include ''the substance'' of the ''Safeguarding'' (-7012) clause in flowdowns. *Compare* DFARS 252.204-7012(m)(1) (Dec. 2015) *with* DFARS 252.204-7012(m)(1) (Aug. 2015).

Small businesses in the DoD supply chain are at risk if they are unable to recognize or report on cyber incidents affecting CDI or do not have the means to affordably and timely implement new cyber security requirements. A recent GAO Report focuses attention on the importance of small businesses to DoD procurement and how little is being done to share cybersecurity resources with them.[6] In fiscal year 2014, DoD obligated approximately $55.5 billion to small business prime contractors.[7] Yet, the GAO found that there is no central repository of federal cybersecurity resources that could be leveraged by DoD's Office of Small Business Programs to share with defense small businesses.[8] The GAO focuses mostly on resources that could help small business with training, outreach and education. Unfortunately, improving these functions, while desirable, will not be enough to enable DoD's small business partners to comply with either the reporting or substantive cyber safeguards requirements of the 'Network Penetration' DFARS.

NIST SP 800-171 is a carefully crafted document that takes a high level, goal-oriented approach to system and information security. It is flexible, rather than prescriptive, and has been prepared specifically for use by contractors who use controlled unclassified information on their own, ''nonfederal'' information systems. Even so, SP 800-171 is not without its rigors. Even a cursory

[4] *Network Penetration Reporting and Contracting for Cloud Services* (DFARS Case 2013-D018), FAQs and PGI, *available at http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services.pdf*. The FAQs indicate that it is the responsibility of the ''controlling DoD office'' (in most cases the requiring activity) to ''[d]etermine whether relevant technical information to be furnished by the Government and/or developed by the contractor contains unclassified CTI [Controlled Technical Information].'' *Id*., at pp. 8-9.

[5] The federal government may obtain export-controlled information from its contractors. Where it does, it may provide that information to other companies or nonfederal parties eligible to receive such information. It is appropriate to apply cyber protection mandates to private contractors or others who are provided such export-controlled information by the federal government. It is neither appropriate nor necessary to apply these strictures to export-controlled information that contractors create or employ but do not deliver to the government.

[6] *Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses*, Rept. GAO-15-777, Sept. 2015 (''GAO Small Business Report'').

[7] *Id.*, at p.1.

[8] *Id.*, at p.3.

examination of the control requirements indicates that, for many businesses, completion of a self-assessment against SP 800-171 requirements will be difficult, expensive and time-consuming. As revised, the 'Network Penetration' DFARS affords companies 30 days to report on SP 800-171 controls they do not meet. All that some companies will be able to do within this time is to report that they presently conform to none of the SP 800-171 requirements. Although allowed by the revised Rule, and despite the final ''due date'' of Dec. 31, 2017, it will be difficult for small businesses to comply with reporting and safeguards requirements without help.

There are fourteen families of controls in SP 800-171. Each is accompanied by several ''Basic Security Requirements'' and most also have additional ''Derived Security Requirements.'' In every case, both ''Basic'' and ''Derived'' requirements are stated in a single sentence or phrase.[9] Substantial technical knowledge may be required to understand the purpose of each Basic or Derived Requirement and even more expertise will be needed to assess and compare these requirements against whatever cyber protection measures may be in place for a given business. Many businesses subject to this Rule will not have systems already in place that cover all the fourteen control families, much less all of the 30 Basic Security and 79 Derived Security Requirements. Nor will they have resources in-house to conduct this analysis. They may not have the financial means to hire outside experts or, worse, they may conclude it is not sound business to invest and incur recurring costs of compliance with these safeguards.

DoD and its higher tier contractors must act to address this problem. It is neither possible nor prudent to exclude small and commercial businesses from the DoD supply chain, but it is equally undesirable to expose CDI to risk of exfiltration and compromise when it is used by these businesses. Pushing the reckoning off two years gives companies more time to comply, but does not necessarily give them the means to comply. New initiatives may be needed. DoD may need to fund and sponsor expert resources to assist small businesses with compliance. Primes may need to act as mentors or provide systems to enable controlled access to CDI for their small business suppliers. New solutions may be offered by third parties to host, transmit and protect CDI, in compliance with the DFARS, where small business users can ''subscribe'' to such services, for purposes of access to and use of CDI, without making individual investment in their own systems.

What Impact Will the DFARS Have Upon Access to COTS Sources?

Another key concern is whether the 'Network Penetration' DFARS applies only if a supplier (at any tier) receives CDI or is put under contract to develop or supply it. The second Interim Rule responds to the concern, as it now states that flowdown is required ''only to subcontractors where their efforts will involve [CDI]'' or where they provide ''operationally critical support.'' 80 Fed. Reg. 81474; *see* DFARS 252.204-7012(m) (Dec. 2015) (clause required where subcontract performance involves a ''covered contractor information system'' which, as defined, is a system that ''processes, stores or transmits'' CDI). The revised Rule, however, does not accommodate circumstances where commercial or COTS suppliers refuse to or cannot comply. For reasons similar to those that should motivate DoD to deal with objections from small businesses, DoD also needs to work with COTS and commercial sources, to prevent them from abandoning the defense supply base.

As suggested above, one key step will be to refine treatment of export-controlled information so that it is not *per se* subject to the 'Network Penetration' DFARS irrespective of whether it is delivered to the federal government. DoD needs to do more, however. It should authorize its Requiring Activities and Contracting Officers to evaluate the information assurance risk presented by use of a given COTS or commercial supplier. Elements of that analysis include threat, vulnerability and consequence. The Government also may consider also whether program objectives can be achieved without disclosing CDI to a COTS or commercial source. Alternatively, evidence may be present that a COTS or commercial supplier has a robust information protection program, even if configured without reference to SP 800171, in which case the source could be accepted by reason of comparatively low ''vulnerability.'' Along these lines, there may be comparatively low impact to *federal* interests should there be a compromise to the integrity of CDI held by a commercial or COTS supplier. Contracting officers should be authorized to approve the continued use of these suppliers, based upon such risk-based analysis. Companies subject to the DFARS should be authorized to conduct similar analyses, limit and control distribution of CDI (where feasible), and determine if there is justification for continuing use of COTS and commercial suppliers. This is a far better outcome than wholesale preclusion of these vital sources of competition and innovation in the supply chain.

How Do Contractors Respond to Solicitations which Contain the DFARS?

The Aug. 26 version of the Interim DFARS required contractors to comply immediately and presented a risk that contractors would be unable to respond to new solicitations that contain the DFARS. The Dec. 30 revision affords contractors additional time, until Dec. 31, 2017, to fully implement the SP 800-171 security requirements. However, the revised Rule also imposes significant new and time-sensitive duties on all defense contractors and their suppliers. As noted, a company must ''represent'' that it will comply with the new cyber safeguards at the time when it *submits* an offer on a *solicitation* that contains the DFARS. DFARS 252.204-7008(c)(1) (Dec. 2015).[10] Also, within 30 days of contract award, companies must ''notify'' the DoD CIO of any SP 800-171 requirements not implemented at the time of contract award. DFARS 252.204-

[9] For example, Basic Security Requirement 3.1.1 for *Access Control* states: ''Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).'' The first Derived Security Requirement, 3.11.2, for *Risk Assessment*, states: ''Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.''

[10] My colleague, Brian Miller, has written an article that examines the potential exposure of contractors to liability under the False Claims Act that conceivably could arise from such representations of compliance. *The Hidden Cybersecurity Risk for Federal Contractors*, Federal Computer Week, Jan. 12, 2016, at https://fcw.com/articles/2016/01/12/miller-oped-false-claims.aspx.

  PVLR ISSN 1538-3423

7012(b)(1)(ii)(A) (Dec. 2015). Mandatory cyber incident reporting is required upon agreement to a contract with the ''Safeguarding'' (-7012) contract clause. Considering what is *not* postponed – ''adequate security,'' notification of SP 800-171 ''gaps'' and incident reporting –obligations arise immediately upon receipt of a contract subject to the 'Network Penetration' DFARS. These will present significant transition issues, notwithstanding the Dec. 30 revision.

DoD may need to re-think what it requires of contractors who respond to solicitations that obligate cyber protection of CDI. The second Interim DFARS requires notification to DoD of SP 800-171 requirements that are not met. This may be one or two steps further than what is immediately practicable. For many companies affected by this Rule, the first necessary step would be to conduct a cybersecurity self-assessment and to prepare a plan of action. Arguably, this is both more realistic and more beneficial, to DoD and its contractors, than the present requirement that focuses upon identification and notification of ''exceptions'' to SP 800-171 requirements. The ''gap'' analysis (versus SP 800-171) would be a byproduct of the self-assessment and figure into the plan of action. ''Adequate security'' will be achieved over time, upon execution of the plan of action.

Which Cyber Practices Are Compliant with SP 800-171?

The Aug. 26 Interim DFARS is confusing in its failure to clearly distinguish among (i) a ''deviation'' from SP 800-171 requirements, (ii) a determination that a requirement is ''not applicable,'' and (iii) consideration of an ''alternative control.'' The Dec. 30 revision does not resolve this confusion. Nor does it clarify how much responsibility resides with contractors to self-determine which cyber measures will be sufficient.

Under the latest version of the ''Compliance'' (7008) solicitation clause, an offeror that proposes to ''*vary* from'' a requirement of SP 800-171 must submit an explanation that an ''authorized representative'' of the DoD CIO is to ''*adjudicate* . . .in writing *prior to* contract award.'' The companion ''Safeguarding'' (-7012) clause, however, differs. It obligates a contractor to provide ''adequate security'' which is either the security requirements of SP 800-171 or ''[a]lternative but equally effective security measures,'' where used to ''compensate for the inability to satisfy a particular requirement,'' but alternative measures must be ''*accepted* in writing'' by an authorized representative of the DoD CIO.'' *Compare* DFARS 252.204-7008(c)(2) (Dec. 2015) *with* DFARS 252.204-7012(b)(1)(ii) (Dec. 2015) (emphases added). The ''Compliance'' solicitation clause requires both submission *and* approval, *prior* to award, of any proposal to ''vary from'' a requirement of SP 800-171, while the ''Safeguarding'' clause permits companies to propose ''alternative'' measures subject to approval that can come *after* award. Further clarification is needed in the next revision to the Interim DFARS or by updates to the PGI. More important, DoD should consider whether its best interests would be served by relinquishing some decision authority over selection of controls and giving greater deference to its contractors.

The Dec. 30 revision exhibits ambivalence as to what role DoD will assert in oversight and approval of contractor cyber protection measures. It should be within the authority of contractors to determine the applicability of each requirement of SP 800-171 as well as whether they have chosen sufficient methods or elected suitable alternatives.[11] A presumption of sufficiency should attach where a contractor completes a self-assessment and prepares a cybersecurity plan of action. DoD can review such a plan, but its role should encompass guidance and consultation, rather than assuming the obligation to ''adjudicate'' or ''approve'' what may prove to be a very long list of variations or alternatives from numerous suppliers. Many contractors will interpret the second Interim DFARS to *require* submission of any cyber protection measure that does not square perfectly with the Basic and Derived requirements of SP 800-171. This risk is aggravated by the flexible nature of SP 800-171; since it is decidedly *not* proscriptive and because each requirement is stated in summary rather than in detail, *by design* SP 800-171 invites companies to make individual decisions on which security issues they confront and how best to address them. Before the DoD CIO takes on the potentially enormous responsibility of ''adjudicating'' or ''approving'' thousands of variations and alternatives, it ought to encourage its contractors to make their own decisions, document their findings, and implement their action plans. DoD need not interpose itself as a necessary decision-maker on actions of thousands of companies whose cyber measures will be tailored to their particular business and risks. Unless DoD accepts a restrained role, and accepts the strategic value of forbearance as industry comes to grip with contractually required cybersecurity, it may become an obstacle to security progress, not an enabler (as it intends).

Comments to the latest Interim Rule are due on or before February 29, 2016. 80 Fed. Reg. 81472. Considering all the open implementation questions as well as areas of apparent conflict within the Rule at present, interested parties should consider making submissions. The community affected by the 'Network Penetration' DFARS is very large. DoD will benefit from the insight of industry at all levels about practical problems they anticipate or have experienced and how to solve them.

---

[11] In the FAQs published in Nov. 2015, DoD points to three relevant provisions from NIST SP 800-171, i.e., 3.11.1 (Risk Assessment), 3.12.1 and 3.12.2 (both, Security Assessment). FAQs, n.6 *supra*, at 14. These are consistent with the proposition that contractors have substantial authority within SP 800-171 to determine measures to correct deficiencies and reduce or eliminate vulnerabilities.