Bloomberg BNA

Federal Contracts Report™

Cybersecurity

Learning to Live with the 'Network Penetration' DFARS

BY ROBERT S. METZGER

The Department of Defense (DoD) held an ''Industry Implementation Information Day'' on Dec. 14 to address questions about the implementation of the Interim Rule, *Network Penetration Reporting and Contracting for Cloud Services*, (DFARS Case 2013–D018) (hereafter, the ''Network Penetration DFARS''), 80 Fed. Reg. 51739, 8/26/15. Even though the new Interim Rule revises a previous rule published in November 2013,[2] reaction from some quarters has been hostile. DoD's presentation at the public meeting is now available online.[3]

Among the chief concerns expressed are these:

- Implementation should be postponed;
- Companies should only be required to safeguard information that the Government has specifically identified as subject to required cyber safeguards;
- Small businesses will not be able to comply with the rule;
- Commercial off-the-shelf (COTS) and commercial sources will refuse to comply with the rule;
- Contractors are unsure how to respond to solicitations that contain the new requirements; and
- Industry is not informed how to determine or establish compliance with SP 800-171.

This article reviews these six key concerns. Recommendations are offered on what industry should do — to ''live with'' the Network Penetration DFARS — and what DoD should do, to respond to industry concerns and improve implementation.

What This Rule Does. Briefly, the Network Penetration DFARS has five principal purposes. First, it expands the **coverage** of the earlier regulation. Now, four information types, collectively ''covered defense information'' (''CDI''), are to be protected. These are ''controlled technical information'' (with military or space application),[4] critical information (operations security), export-controlled information and ''[a]ny other information''

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

[3] Slides presented by DoD officials at the December 14, 2015 meeting are available at http://www.acq.osd.mil/dpap/pdi/docs/Industry_Implementation_Information_Day_(Dec_14_2015%20)_Slides.pdf.

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.

[4] What was Unclassified Controlled Technical Information (UCTI) under the earlier regulation is now ''controlled techni-

that requires safeguarding or dissemination controls pursuant to ''laws, regulations, and Government-wide policies.[5] Second, the rule changes the **safeguards** to use for information security, using the new NIST SP 800-171[6] as the basis for cyber controls to protect CDI,[7] rather than a table of controls derived from NIST SP 800-53, as was applied by the UCTI Rule. Third, the rule now requires **flowdown** to all subcontracts. Fourth, the rule clarifies procedures for **cyber incident reporting** and now includes measures intended to encourage reporting that will limit the use or disclosure of third-party cyber incident information. Fifth, the rule includes new provisions when DoD is acquiring **cloud** services. The rule is immediately effective.

Why This Rule Is Necessary. The purpose of the Network Penetration DFARS, and the UCTI Rule that preceded it, is to protect sensitive but unclassified DoD information that resides on contractor networks. Each of the four forms of CDI represents information that potential adversaries — governments, non-state actors, or even commercial rivals — have sought and obtained through cyber exfiltration. Compromise of this information has many adverse consequences to national security. This risk is not conjectural, as there are documented instances where theft of valuable technical data from U.S. contractors has accelerated the ability of rivals to approach or match our capabilities. Considerable challenge is present, as data security has supplanted physical security as the objective for sensitive and valuable information.

Issue 1: Implementation Should Be Postponed. Some critics contend that the rule comes as a surprise to industry and that its implementation should be postponed until after further notice-and-comment rulemaking or input from stakeholders. DoD for many years has sought to improve the level of information security in the defense industrial base. Back in 2011, DoD first published a proposed rule to implement adequate security measures to safeguard unclassified DoD information within contractor information systems from unauthorized access and disclosure.[8] The UCTI Rule, which shares the essential purpose of protecting sensitive DoD information in the hands of its contractors, was promulgated and made binding as an Interim Rule in November 2013. DoD has regularly consulted with participants in its Defense Industrial Base (DIB) Cybersecurity and Information Assurance Program (CS/IA) about the objectives and operation of the rule. The threat to the confidentiality of sensitive federal information is active and cannot be postponed. Considering the rulemaking history, implementation should not be deferred. By publishing this as an Interim Rule, DoD seeks to improve uniformity of application by DoD components and Requiring Activities. But DoD can *improve* implementation, as explained below, to address some industry objections.

Issue 2: Identification of Covered Defense Information. Industry is worried that it won't know what information it is required to protect. DoD appears to accept that it has the responsibility to designate and identify information that is CDI. Generally, DoD is to follow Department of Defense Instruction (DoDI) 5230.24, issued on Aug. 23, 2012. Its purpose is to establish a standard framework and markings for managing, sharing, safeguarding, and disseminating technical documents. The DoDI states, at Section 2.a.(2), that ''[a]ll newly created, revised, or previously unmarked classified and unclassified DoD technical documents shall be assigned'' one of six Distribution statements (''A'' through ''F''), only one of which (''A'') denotes documents approved for public release. Industry may also be informed by provisions in the solicitation. In some cases, DoD will contract for the development of data which, once delivered, will be controlled. In this situation, contracts will include a Contract Data Requirements List (''CDRL''), DD Form 1423, in which the Requiring Activity is to indicate, in Block 9, whether a ''Distr[ibution] Statement [is] Required.'' Thus, if the DoDI is followed, and Contracting Officers (''COs'') are attentive to the CDRL content, contractors will know when they receive or create information subject to the required safeguards. As a DoD official explained at the Dec. 14 meeting, a contract should clearly state when it involves CDI.

In the real world, however, government officials may overlook DoDI designation obligations or fail to identify the applicable Distribution Statement in CDRL Block 9. In some cases, companies will have a sufficient basis to conclude that information nonetheless should be subject to safeguards. They can apply such measures, even if technically unnecessary, to avoid the risk of noncompliance. If unsure about particular data, a company should ask for direction from the CO. As a general proposition, however, companies should not be liable, contractually or otherwise, where they exclude from safeguards information that DoD did not designate as CDI. (Exceptions could be present where it is manifestly unreasonable, under particular circumstances, not to protect information.) It is DoD's responsibility to inform contractors when it provides them CDI or contracts with them to furnish CDI.

Issue 3: Small Businesses Will Not Be Able to Comply. Small businesses are an important and sometimes required part of the defense supply chain. In the promulgation comments accompanying the Network Penetration DFARS, DoD acknowledges that the rule may have a ''significant economic impact'' on a ''substantial number'' of small businesses, and It estimates the rule may apply to 10,000 contractors, less than half of whom are small businesses.[9] The rule invites the comments of small business — but does nothing to assuage their concerns.

Larger businesses, even if their principal focus is upon commercial markets, are likely to have some form

---

cal information,'' one of the four types of CDI. DFARS 204.7301 (Definitions), at 80 Fed. Reg. 51742.

[5] The last category anticipates the final rule on Controlled Unclassified Information, which is being prepared by the National Archives and Records Administration (NARA). *See Controlled Unclassified Information*, (Proposed Rule), 80 Fed. Reg. 26501, May 8, 2015, available at http://www.gpo.gov/fdsys/pkg/FR-2015-05-08/pdf/2015-10260.pdf.

[6] *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, NIST Special Publication (SP) 800-171, June 2015, available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf.

[7] DFARS 252.204–7008

[8] *Safeguarding Unclassified DoD Information* (DFARS Case 2011–D039), (Proposed Rule), 76 Fed. Reg. 38089, June 29, 2011.

[9] 80 Fed. Reg. 51740.

  FCR ISSN 0014-9063

of cybersecurity in place. They can assess what they have against SP 800-171 and come up with a plan to close gaps. Small businesses, however, may start without any cyber protection and they are less likely to have the necessary security resources in-house. Self-assessment, implementation of cyber safeguards and provisioning to report cyber events will be costly. DoD has not answered this problem sufficiently, but it must. There are several possibilities. First, DoD should explore creation of a special Small Business Cybersecurity Support Center — to provide no-cost assistance to qualifying small businesses. This might be done in conjunction with the Small Business Administration. Second, DoD should encourage its prime and higher tier contractors to ''mentor'' their small business partners and, where possible, allow those companies to provide required security for the CDI that may be needed periodically by the small business. Third, DoD should develop guidelines that enable its small business suppliers to outsource and use third parties to host and protect CDI. One can readily envision that small companies will hire cloud service providers to host, control and protect CDI — but DoD thus far has not provided any instruction or authorization for this practice.

Issue 4: COTS and Commercial Sources Will Refuse to Comply. The Network Penetration DFARS applies broadly to DoD contractors and subcontractors to provide adequate security to safeguard CDI from unauthorized access and disclosure. A solicitation provision, DFARS 252.204-7008, is to be included in all solicitations and contracts, including those using FAR Part 12 procedures for the acquisition of commercial items.[10] The -7008 clause operates to apply safeguarding requirements, relying upon NIST SP 800-171, where CDI is on an information system that is owned, or operated by or for, a contractor. Where the clause is present in a DoD solicitation, or is flowed down to a subcontractor, suppliers of COTS products and other commercial sources may object. Even though defense may be no more than a very small fraction of their business, they are being forced to implement controls specific to DoD and to accept liability exposure should there be compromise of CDI subject to the rule. Higher tier DoD contractors worry that commercial and COTS suppliers will refuse to sell to them.

Initially, the risk may not be as great as some surmise. The Network Penetration DFARS applies only if a supplier (at any tier) receives CDI or is put under contract to develop or supply it. Very likely, a high proportion of subcontracts with COTS and commercial sources will not involve CDI. In such case, even if the clause is referenced in a purchase order, it will have no effect since the necessary predicate — CDI — is not present. This is not enough assurance, however. Particularly because the rule now includes export-controlled information as one of the four forms of information that comprise CDI, there will be many ''downstream'' awards to commercial companies that supply products or technology that may be subject to export rules and therefore could fall within this category of CDI requiring cyber safeguards.

DoD should be alert and responsive to situations where its access to commercial sources in its supply chain is imperiled by the new rule. DoD should create a procedure to enable its suppliers to inform Contracting Officers (or Requiring Activities) where supplies are acquired from commercial or COTS suppliers who decline, in whole or part, to accept the flowdown. In certain circumstances, there will be no available alternative or cost-effective choice other than to proceed with a particular COTS or commercial source. There may be surrogate measures that will protect CDI provided by covered contractors to COTS and commercial sources, such as retention of the data by the higher tier contractor or use of encryption or digital rights management technologies that protect sensitive data at the information level rather than at the information system level. Exceptions to flowdown also could be provided where the only CDI at issue is the contractor's own export-controlled information, on the theory that the contractor has separate obligations, under the relevant export control regimes, to protect such information against unauthorized access.

Issue 5: Contractors Are Unsure How to Respond. The new rule will appear immediately in new solicitations and we can expect DoD to seek to add the DFARS CDI protection measures to existing contracts by bilateral modification. Pursuant to DFARS 252.204-7012(b), contractors are obligated to provide ''adequate security'' for all covered defense information. Concerning contractor information systems, the ''minimum'' requirement refers to NIST SP 800-171 unless the contractor receives approval of alternative, but equally effective measures. Transition measures are notably absent from the rule, however. This presents an immediate problem for both DoD and for its contractors. A company now may receive a solicitation with the DFARS ''adequate security'' and SP 800-171 requirements. Even if that company has cybersecurity protections in place, it will take some time to conduct a ''fit/gap'' analysis of how well existing controls measure up against SP 800-171 and what is needed to close gaps or resolve questions. Even more time will be needed if communications are necessary to the Requiring Activity, or if it is necessary to engage the DoD CIO's office to consider alternative measures. And still further time will pass while contractors implement measures indicated by the ''fit/gap'' analysis or as informed by DoD officials.

This challenge is further complicated. SP 800-171 is not prescriptive. Rather, it states performance requirements, at a high level. This differs greatly from the specifics and mechanics that can be found in NIST SP 800-53, from which the UCTI Rule selected and mandated controls and enhancements. A crucial benefit of the SP 800-171 is its flexibility and ability to accommodate many different strategies and methods to achieve performance goals. But uncertainty accompanies this flexibility — because the absence of enumerated requirements means that judgment necessarily must be applied to fashion controls to address particular security risks and business circumstances. And, beyond this, the DFARS contains no mechanism of any kind by which any contractor can secure review and approval of its system of cyber safeguards and controls for CDI. As explained at the Dec. 14 meeting, when a company signs a contract subject to the DFARS, it is ''self-attesting'' to its compliance. Necessarily, there is a discontinuity if a Requiring Activity expects immediate compliance with the DFARS, at the time of proposal submission, but the contractor requires more time before it can ''self-attest'' on

[10] DFARS 204.7304, 80 Fed. Reg. 51743.

an informed basis. In its present form, the DFARS makes no provision either for time or process for implementation.

DoD needs to answer this problem, and soon, or else it will find that some contractors are unable to respond to new solicitations that contain the DFARS. It may be necessary to address transition issues by further changes to the Interim DFARS. There are measures that can be taken as matters of contractor oversight and contract administration. (As these are developed, they should be shared, among Requiring Activities and Contracting Officers, and added to the ''Frequently Asked Questions'' (FAQs) document that DoD already has produced.[11]) One of the Basic Security Requirements of SP 800-171, at 3.12.1, is that organizations ''[p]eriodically **assess** the security controls in organizational information systems to determine if the controls are effective in their application.'' At 3.12.2, organizations are to ''[d]evelop and implement **plans of action** designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.'' These controls could serve as the starting point for implementation. Solicitations could ask contractors to conduct a cybersecurity self-assessment and to advise of their planned improvements. Receipt of the documented results would improve the confidence of Requiring Activities that offerors in fact will meet the new obligations to protect CDI. This new rule is being applied across the whole span (and depth) of the DoD supply chain. It is reasonable during a transition period to determine that ''adequate security'' is present where a company has documented and (if requested) submitted its self-assessment and plan of action. If appropriate, contract terms can be added to require submission of progress reports. Such periodic updates would align with another important feature of the DFARS — namely, the obligation, imposed by the rule, that contractors must ''[a]pply *other* security measures (beyond the SP 800-171 baseline) when such measures ''may be required to provide adequate security in a dynamic environment.'' As to CDI as well as other data to be protected against cyber threats, effective security is not a static, ''check the box'' exercise.

Issue 6: What Is Compliant? As suggested above, uncertainty is an unintended byproduct of the flexibility of SP 800-171. Contractors appreciate that there is no authentication or approval process for the cyber safeguards they implement to satisfy the DFARS. But they also will be wary of signing up to contracts that contain obligations that are open-ended (''adequate security in a dynamic environment'') in the context of a cyber universe characterized by persistent and ever-changing threats. Only a foolish company would presume that it will not suffer a cyberattack that could compromise the confidentiality of CDI. The new regulation tries to assuage liability concerns. It states:

A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate information safeguards for covered defense information on their unclassified information systems, or has otherwise failed to meet the requirements.

DFARS 204.7302 (d). But contractors also know that the rule requires them to promptly report cyber incidents to DoD. They must assume that DoD will investigate reported events. The level of scrutiny will increase as a function of impact. If especially large quantities of highly sensitive information are compromised, a very thorough probe is all but certain. Thus, it will be after a cyber event that the Government comes to evaluate, or even judge, the adequacy of each contractor's safeguards. Every prudent company will want as much advance assurance as possible that its system, if or when scrutinized, will ''pass.'' Getting this assurance will be difficult, in part because of the flexibility of the control regime, and in part because there is no validation process.

Here too, the Network Penetration DFARS has constructive elements, but needs improvement. The -7008 clause provides that offerors, if they decide to ''deviate'' from SP 800-171, can submit to the Contracting Officer, for consideration by the DoD CIO, a written explanation of:

- why a particular security requirement is not applicable; or

- how an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

DFARS 252.204-7008 (c). It is positive that the rule provides this ''consultative'' mechanism and that the CIO's office is involved. This will greatly improve the likelihood of consistent answers. But it is not enough.

First, DoD needs to fix the Network Penetration DFARS to resolve and clarify when companies need to go to the Contracting Officer, or the CIO's office, for guidance. By design, SP 800-171 is flexible, permitting many strategies and methods to achieve its performance goals. Among the Basic Assumptions stated by SP 800-171, at 2.1, are these two:

- Nonfederal organizations can implement a variety of potential security solutions either directly or through the use of managed services, to satisfy CUI security requirements; and

- Nonfederal organizations may not have the necessary organizational structure or resources to satisfy every CUI security requirement and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a particular requirement.

Considered in context, the present ''consultative'' mechanism is confusing. The boundaries that separate a ''deviation,'' a determination that a requirement is ''not applicable,'' and consideration of an ''alternative'' control, are obscure. Moreover, the role reserved by the CO and the CIO's office, upon examination, is contrary to the assumptions on which SP 800-171 safeguards are built. Readers will see that the language used in the DFARS, requiring DoD CIO approval of ''alternatives,'' is the same as that in the second of the cited SP 800-171 assumptions. It should be within the authority of *contractors* to determine the applicability of each ''Basic'' and ''Derived'' Security Requirement of SP 800-171. It should be equally within the authority of *contractors* to

[11] Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013018) Frequently Asked Questions (FAQs), Nov. 17, 2015, available at www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services.pdf.

   ISSN 0014-9063

determine whether alternatives are appropriate. It works against the premise of SP 800-171 to obligate contractors to submit and seek permission, and it likely will prove to be another source of delay and frustration.

The better way, potentially, is to focus upon *disclosure* of these decisions, i.e., on requirements deemed inapplicable, or on suitable alternatives. Such disclosure, naturally, could accompany the self-assessment and action plan suggested above. There is a role for Contracting Officers and the DoD CIO's office. After reviewing contractor submissions, COs could refer any questions to the CIO's office for response. Similarly, contractors should have opportunity — but not the obligation — to query the CO and obtain CIO response. The query and response process should be available, but not mandatory. Further, companies should receive assurance based upon their good-faith efforts. If a contractor completes a self-assessment and plan of action, and documents its decisions as to applicability of requirements and alternatives, it should be entitled to a presumption of sufficiency and compliance. Should a cyber incident nonetheless occur, there may be later investigation. For purposes of such investigations and enforcement, that presumption should hold, protecting the contractor against liability or sanction, unless there is positive evidence of bad faith, reckless behavior or deliberate acts to mislead the government. A company, for example, could be punished if it promises to take cybersecurity measures but deliberately fails to do so. But it could not be punished if it shows good-faith efforts to perform in accordance with its self-assessment and plan of action, or for its decisions, on applicability or alternatives, absent direction from the CO to act otherwise.

Conclusion. DoD is to be commended for its willingness to meet with stakeholders and explain its intentions regarding the Network Penetration DFARS — even if the meeting occurred after the Interim Rule became effective. Without question, the DFARS serves important and urgent national purposes. Improving cyber safeguards and cyber incident reporting for the whole of the defense supply chain, however, is a very large and complex undertaking where no one today can anticipate bona fide implementation issues that will confront industry as it seeks to comply. DoD occupies a leadership position among federal agencies, and its experience with the Network Penetration DFARS will be important guidance to NARA, the Office of Management and Budget, GSA and other agencies as they work to extend cyber protection to all the categories of Controlled Unclassified Information that will be the subject of the NARA CUI rule, when it is finalized. DoD should rapidly act to address transition and compliance issues, to make achievement of its cybersecurity objectives both workable and affordable.