**The Cyber DFARS: Key Questions, Asked & Answered**
**Part II**
by Robert S. Metzger

This is Part II of the analysis prepared by Robert Metzger,[i] of Rogers Joseph O'Donnell, P.C. (RJO), of the DoD's cyber contract clause, DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." This DFARS requires contractors to implement NIST SP 800-171 cyber safeguards by December 31, 2017.

This analysis is furnished to inform readers of the author's opinions on how the DFARS should be applied. It does not constitute legal advice and does not establish an attorney-client relationship.

1. **APPLICATION**: Does the DFARS apply to information that has been accumulated over years or which is used for business systems or performance management?

As a general proposition, the answer is "no" – and for several reasons. First, as a matter of contract law, the DFARS imposes obligations only from the point in time that a company accepts a contract in which the clause is included. Second, it is DoD's responsibility to "mark, or otherwise identify in the contract, any covered defense information that is provided to the contractor." DPAP Memorandum, Sep. 21, 2017, p.1 at http://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf. Third, DoD officials have stated publicly that "covered defense information" is not meant to include a contractor's internal information, e.g., human resource or financial, that is "incidental to contract performance." Although I am confident in this conclusion, language in the DFARS definition of "CDI" contributes to uncertainty. The -7012 DFARS says that information used "in support of the performance of the contract" can be CUI. The phrasing is susceptible to expansive interpretation – as, conceivably, any information with even a remote connection to a contract might be thought to be "in support of" its performance. That result would be expensive, unwieldy and unpredictable. And it would not contribute to achievement of security for information that matters most. DoD is obligated to submit annual reports to Congress regarding cost, schedule and performance of each major information technology investment program. 10 U.S.C. 2445b. Enhanced security for CDI requires investment by the DoD industrial base. Implementation of CDI safeguards, and oversight by DoD, should consider cost, schedule and performance impact upon the defense industrial base. This is a further reason to interpret the DFARS to *require* protection of information *designated by* DoD as CDI. A contractor might elect to extend cyber safeguards to similar information not so designated – but that is not a requirement of the DFARS or SP 800-171.

2. **APPLICATION:** What are some of the common risks and challenges encountered with supply chain compliance?

Flow-down is mandatory, at all levels, excepting COTS items but including purchases from commercial sources. DoD officials have publicly described flowdown as a requirement that "must be enforced by the prime contractor." From a threat and outcome perspective, DoD's position is understandable. Adversaries target smaller companies in the supply chain where security may not be as good and where valuable data may be easier to find and extract. From an implementation standpoint, unfortunately, actual improvement of supply chain security is difficult to achieve. It is easy enough for prime contractors to include the cyber DFARS in flow-

down T&Cs, but not so easy to assure compliance. Some subs may refuse, others may qualify their acceptance, and some might promise compliance but not take the necessary actions. Some DoD officials, presented with this situation, respond that the higher tier company should refuse to do business with the reluctant sub, or limit the information shared with the sub. That is not always a workable solution. Subcontractors include small businesses which offer unique capabilities, established and trustworthy relationships, and can be the source of desired innovation. Other sources that balk at the DFARS or NIST requirements may be commercial concerns, or international suppliers. They may refuse to accept contract responsibility to satisfy the DFARS and NIST, even though they may follow strong security practices. The prime is in a tough spot. It has little leverage but considerable exposure. It is the prime that has privity of contract with the Government. Should there be a cyber breach in the supply chain – and assuming that the breach is reported, as the DFARS requires – the Government's legal rights extend only to the prime and not to the upstream suppliers. Solutions will not be easy to come by, or free.

3. **APPLICATION:** How can the Government, or prime contractors, assist commercial suppliers, small businesses, and other partners to comply?

Telling prime contractors to look elsewhere if an intended supplier declines the DFARS is an unsatisfactory solution. In the "worst plausible case," the result would be to stop the development or supply of a military item because an indispensable subcontractor cannot or will not accept the flow-down. There could be unacceptable consequences to price, schedule and performance. Case-by-case measures may be necessary. There are a number of measures to consider. In the most extreme situation, the prime should contact the Contracting Officer, Program Office or Requiring Activity, and involve the DoD CIO's office if necessary, to agree upon an acceptable risk-informed alternative. Primes also can mentor subs and provide security training and resources. There are potential technical solutions, such as having the prime provide managed security "as a service," essentially relying upon the prime to host and secure CDI and limiting access and use rights by the subcontractor. More generally, many smaller businesses will seek to increase use of the cloud for security rather than invest in DoD-specific on-premises improvements. (DoD needs to facilitate rather than frustrate this outcome.) Also, DoD and other Government agencies are working to improve tools and resources to help smaller businesses. DoD and NIST are soon to release guidelines helpful to the manufacturing sector through the "Manufacturing Extension Partnership." https://www.nist.gov/mep Through the Defense Logistics Agency (DLA), DoD also is suing its Procurement Technical Assistance Program (PTAP) to provide implementation help, especially for small businesses. http://www.dla.mil/HQ/SmallBusiness/PTAP.aspx.

4. **APPLICATION:** Are international suppliers subject to the DFARS? How does the DFARS treat "export controlled" information?

Yes, international suppliers are subject to the DFARS. The flowdown requirement is not limited to U.S. supply chain partners. Defense supply is dependent upon a global supply chain. And international suppliers are likely to resist or reject the DFARS and SP 800-171. In many situations, there is no "work around" or supply alternative. Faced with this situation, DoD contractors must work with Government to reconcile security objectives to practical constraints.

The U.S. contractor should not suffer risks outside its control. Export controls and mandatory cyber safeguards are less similar than they may appear initially. NARA's CUI "Registry" includes export-controlled information as a CUI category. By definition, export-controlled information is that which U.S. policy, law and regulation protects against unauthorized foreign disclosure. Export control laws include means to selectively authorize foreign access. The cyber DFARS seeks to protect information against cyber exfiltration, irrespective of any intent to export, and regardless of the presence of an export license. Where possible, a U.S. contractor should apply cyber safeguards to export-controlled data just as it protects all forms of CDI. Both public and private interests are served. But this outcome is *not* mandated by the DFARS regulation. The DFARS applies to information which DoD provides or purchases that it designates as CDI. It does not apply to export controlled data that exists independent of any government contract. Companies routinely use export-controlled data, that they did *not* receive from the Government, and which they do *not* deliver to the Government, to produce supplies or deliver services to the Government. Such information is not "CDI" and is not subject to the DFARS or to SP 800-171 even if it all parties would benefit from equivalent cyber protection. It is a *business* decision whether to apply cyber protection to company information that is export-controlled; it is a *contractual* (and legal) obligation to protect that information when it is marked or otherwise identified by the Government as CDI.

5. **ACQUISITION:** How can compliance impact contract eligibility, evaluation or award?

DoD has made available "Frequently Asked Questions" (FAQs) which discuss this subject. http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf. (DoD is working on an update to these FAQs.) It states that the DFARS clause is not structured to require contractor compliance with SP 800-171 as a mandatory evaluation factor. However, "the requiring activity is not precluded from stating in the solicitation that it will consider compliance" in the source selection process. Several examples of how a requiring activity might proceed are provided. This subject receives further attention in the Sep. 21 DPAP Memorandum. It advises that the requiring activity must state in the solicitation whether and how it will consider the contractor's implementation of SP 800-171. If cited in proposal instructions, and referenced in sections L and M of a solicitation, a requiring activity can request and evaluate the adequacy of a contractor's security measures. A solicitation may request the contractor's SSP for DoD to determine whether it is acceptable or unacceptable. Compliance with the DFARS -7012 clause can be established as an evaluation factor, provided that offerors are so notified and informed of how the evaluation will proceed. A requiring activity can require offerors to identify -171 requirements not met at the time of award and hold the contractor accountable to meet the requirements in accordance with its own plan of action. A contractor's SSP and plan can be incorporated by reference into the contract. In other words, DoD has reserved to itself, and clearly signaled to industry, that it can and in some cases will assess the adequacy of DFARS compliance in the source selection process. Companies working on high impact DoD programs should anticipate DoD evaluation of their cyber compliance, and the SSP and plan of action.

6. **ACQUISITION:** Can cybersecurity compliance factor into bid protests?

Yes. As indicated above, we can expect to see more procurements where DoD customers review, approve, assess and score a contractor's security. There may be pre-award protests where potential bidders object to requirements as unnecessary, overly restrictive, or impermissibly vague. Pre-award protests may be filed where would-be offerors are excluded from the competitive range (for example), after a preliminary finding that their security is inadequate. Disappointed bidders may raise several objections in a post-award protest, e.g., that the Government wrongly found their security to be inadequate, unfairly scored their security, or wrongly found that the winner's bid was adequate. Another area likely to prompt dispute is where an offeror is not entirely compliant at the time of proposal submission but the Government accepts its promise of future performance. Just as other areas of performance or regulatory requirements are grist for the mill, it is inevitable that DFARS -7012 compliance, and the adequacy of SP 800-171 implementation, will figure in protests. This places GAO examiners, or Court of Federal Claims judges, into a potentially difficult position. Evaluation of contractor security has national security implications and may involve highly technical issues. Historically, the GAO has given considerable deference to agency actions in such areas. In one decision, it found that "where requirements relate to issues of human safety or national security, an agency has the discretion to define solicitation requirements to achieve not just reasonable results, but the highest possible reliability and effectiveness." *Coulson Aviation (USA), Inc*., B-411525, Aug. 14, 2015, 2015 CPD ¶ 272 at 15 (citing *Womack Mach. Supply Co*., B-407990, May 3, 2013, 2013 CPD ¶ 117 at 3). Agency officials should not be immunized from errors in the appraisal of security that affect competitive opportunity. But deference is due to government personnel in this sensitive, complex area.

7. **ADMINISTRATION:** Are costs incurred from implementation of cybersecurity safeguarding controls to meeting DFARS 252.204-7012 compliance recoverable?

For companies subject to federal contract cost principles (FAR Pt. 31), costs incurred to implement the safeguards required by the DFARS and SP 800-171 are allowable provided that they are reasonable, allocable, and not otherwise prohibited by contract terms. Even though allowable, however, actual *recovery* may be problematic depending on a company's mix of commercial/government work as well as its composition of government contract types. For example, for companies who primarily perform cost-type contracts, the cyber security cost of becoming and remaining compliant will be recovered through incrementally higher indirect cost rates (unless restricted by rate ceilings or funding limits). Conversely, companies who perform primarily long-term and/or highly competitive firm fixed-price contracts will be challenged because contract prices will not be increased to cover all increased costs. Thus, DoD's cyber requirements can produce asymmetric impacts, burdening companies subject to the DFARS with costs not borne by their rivals in commercial markets. This puts DoD suppliers at a disadvantage in other markets. Where DoD is not a large enough end-customer to justify a cyber compliance premium, companies will exit from or be deterred from entry into the defense industrial base. This is an issue that DoD must address. Security comes at a cost. DoD should include funds in new awards that are sufficient to cover the higher security expense of its prime contractors and their supply chain. DoD should include funds in new awards that are sufficient to cover the higher security expense of its prime contractors and their supply chain. And it should work with primes to reduce the expense of maintaining "adequate security.' One

way this can be done, in the author's opinion, is to promote supplier use of cloud-delivered security for many small and medium-sized enterprises, this is less expensive and more effective than on-premises improvements. (Thanks to Patrick Fitzgerald, formerly DCAA Director, presently with Baker Tilly Virchow Krause, LLP, for his insight on this question.)

8. **ENFORCEMENT:** What is the purpose of "cyber incident" reporting and what happens after a report is made?

With all the attention being paid to the "deadline" of Dec. 31, 2017 for NIST SP 800-171 compliance, many companies have given little thought to the *reporting* obligations of the 'Network Penetration' DFARS. They should. Cyber incident reporting is as important as the safeguards. Reporting, a continuing obligation, is important because cyber breaches can and do happen, even with improved safeguards. DoD conducts a damage assessment after a breach, and may take mitigation measures. DoD also seeks to know how the attack was implemented. There are four components to the reporting obligation: (1) the cyber incident report, to be furnished with 72 hours of discovery; (2) submission of malicious software, if isolated; (3) cooperation, should DoD undertake a forensic investigation; and (4) flowdown, to inform DoD of breaches at any supply chain level. Companies should review the DFARS Procedures, Guidance and Instruction (PGI) 204.73, at http://www.acq.osd.mil/dpap/dars/pgi/pgi_htm/PGI204_73.htm. DoD expects contractors to cooperate in the damage assessment. The PGI advises that the Government may assess the sufficiency of a contractor's cyber measures. It may review the SSP to evaluate "whether any of the controls were inadequate, or if any controls were not implemented at the time of the incident." Subcontractors are required to report directly to DoD and to inform their prime (or next higher-tier subcontractor) of the DoD-supplied report number. (The DFARS does not require subcontractors to provide the full incident report to their prime.) Companies subject to the DFARS should not wait until after an incident has occurred to figure out what to do. NIST SP 800-171 contains three discrete safeguards for Incident Response. These require companies to (i) establish an operational capability for incident response and o prepare adequately (Safeguard 3.6.1); (ii) to track, document and report incidents to appropriate authorities (3.6.2); and (iii) test the organizational response capability (3.6.3).

9. **ENFORCEMENT:** What are the likely ways the Government will enforce DFARS 252.204-7012?

The fact of a breach, and the filing of a cyber incident report, itself does not establish that there was any violation of the DFARS or non-compliance with SP 800-171. However, a company can be scrutinized after it submits an incident report. The PGI establishes that there will be a damage assessment after a cyber incident report is filed. Several DoD elements participate, including the requiring activity, contracting officials, and potentially the DoD CIO's office. Law enforcement personnel, such as the FBI, could be involved. Thus, the near term, enforcement actions will be precipitated, if at all, after a reported breach. Companies should not fail to report a cyber incident in the hopes of avoiding scrutiny; to do so would clearly violate the DFARS -7102 obligations and expose the company to serious sanctions. Prudent companies should assume a breach will occur and expect to be evaluated after their incident report. The documented SSP will be critical to demonstration of

compliance. It should be reflect an informed self-assessment. Third party assessment, while not a guarantee, can reinforce the record for review. A company should be prepared to show good faith execution of any plan of action for mitigation and security improvement. Companies should recognize that compliance is neither a one-time event nor a check-the-box exercise. DFARS 252.204-7012(b)(3) states that companies may need to apply additional information system security measures if required to provide "adequate security in a dynamic environment". Over time, we can expect the level of government scrutiny to increase. For example, the DCMA's role is evolving. Initially, DCMA will check whether companies have prepared the SSP and established the specified means to report cyber incidents to DoD. DCMA likely will assume substantive oversight responsibilities as industry and DoD gain experience with the DFARS and SP 800-171 and as DCMA acquires necessary expertise.

10. **GENERAL:** Is today's DFARS as far as DoD will go, or will some DoD customers demand stronger measures? Can we expect anything similar from the civilian agencies?

The present -7012 DFARS and SP 800-171 safeguards treat all forms of CDI as having a "Moderate" impact level should breach occur and confidentiality be lost. Some DoD programs, and some unclassified information on those programs, are more sensitive. The injury to national defense or mission capability could be more severe if a cyber breach conveys more sensitive information to an adversary. Discussion continues within the security community of how to respond. Some suggest "tailored" versions of SP 800-171, "overlays" to the basic safeguards, or even a DoD-specific minimum security statement like the Security Requirements Guide (SRG) that the Defense Information Security Agency (DISA) issued to address DoD's distinct cloud security concerns. Already, requiring activities can evaluate contractor security in an acquisition process. Higher contractual scrutiny of contractor security measures can be expected for high-impact programs. Other themes concern DoD security experts. One is whether to increase protection of information "integrity" and "availability" as distinct from the "confidentiality" focus of the present DFARS and SP 800-171. Another is whether to extend required security to discrete cyber-enabled operations such as defense manufacturing. As to the civilian agencies, FAR 52.204–21 ("Basic Safeguarding of Covered Contractor Information Systems"), promulgated in May 2016, applies to all "Federal contract information" (FCI). It contains fifteen general controls, consistent with those of SP 800-171, which apply to information systems that host FCI. Most important, NARA is leading an active rule-making effort to produce a new "CUI FAR" generally applicable to all civilian agencies. Following on the approach that DoD has taken in the 'Network Penetration' DFARS for CDI, the future FAR rule likely will obligate civilian agencies to secure the confidentiality of all forms of CUI that are made available, by contract or other agreement, to any non-federal partner, inclusive of contractors, state and local governments, universities and other. The expected FAR CUI rule also will rely upon SP 800-171 security safeguards, as this is seen as promoting "consistency" in federal cyber rules.

Your comments and questions regarding this document are welcome. Should you have questions regarding the interpretation, application and implementation of the cyber safeguards required by the DFARS and SP 800-171, or on cyber incident reporting requirements, you may contact Bob and his team at rsm@rjo.com or (202) 777-8951.

[i] Robert Metzger is a recognized subject matter expert in cybersecurity and government contracts. He was named by Federal Computer Week a 'Federal 100' winner in 2016 for his work on the convergence of supply chain and cyber security. As a Special Government Employee of the Department of Defense, Bob is a member of the Defense Science Board task force that produced the Cyber Supply Chain Report earlier in 2017. He has been recognized for cybersecurity expertise and identified as a leading U.S. and international government contracts lawyer by such rating authorities as *Chambers USA*, *The Legal 500* and *Who's Who Legal*. The views expressed here are his own and are not to be attributed to the Department of Defense, the Defense Science Board, to any organization with whom he has worked or is affiliated, or to any client of Rogers Joseph O'Donnell, P.C.