**The Cyber DFARS: Key Questions, Asked & Answered**
**Part I**

by Robert S. Metzger
October 2017

DoD contracts now include a clause, DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," that requires contractors (and much of their supply chain) to implement NIST SP 800-171 cyber safeguards by December 31, 2017. Many companies are struggling to understand and comply with this 'cyber DFARS."

The purpose of this analysis is to assist companies of all sizes to comply with the DFARS – while respecting affordability and resource constraints.

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.

The author is Robert Metzger, an attorney in private practice who heads the Washington, D.C. office of Rogers Joseph O'Donnell, P.C. (RJO), a firm that has specialized in public contract matters for more than 35 years. Bob is a recognized subject matter expert in cybersecurity and government contracts. Among his credentials are these –

- Bob was named by *Federal Computer Week* a 'Federal 100' winner in 2016 for work he's done 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[i];
- Bob 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*.

Bob advises U.S. and international companies of varying sizes and from many industry sectors. This article will draw upon his experience in dealing with both industry and government on cyber compliance matters. Should you have questions, Bob and his team at RJO may be able to assist. He can be reached at rsm@rjo.com or (202) 777-8951.

1. **PURPOSE:** What is DoD trying to accomplish with this cyber rule.

Evidence is strong that adversaries have "exfiltrated" – stolen – valuable tech data from DoD suppliers. This can be the result of nation state espionage, criminal enterprises or even commercial rivals. Such threats continue. DoD's goal is for its entire supply chain to improve protection of the confidentiality of information that is unclassified but nonetheless sensitive – especially technical data. The Pentagon seeks to reduce exposure, stanch data loss, and be informed of successful attacks and their consequence. From an operational standpoint, the DFARS has four purposes: (1) safeguards on information and information systems; (2) prompt detection and reporting of cyber incidents; (3) submission of malicious

software to DoD Cyber Crime Center (DC3) and cooperation in any forensic investigation; and (4) flow down to lower tier suppliers. DoD's principal concern is with "Controlled Technical Information" (CTI), which has military or space significance). DoD also has concerns about other CDI types, such as Personally Identifiable Information (PII), which adversaries could use for "social engineering" or other hostile purposes.

2. **GENERAL:** What must contractors do by December 31, 2017 to be in compliance?

Two DFARS clauses are most important. First, the "Compliance" clause, 252.204-7008, to be included in all solicitations, includes a representation that an offeror "will implement" the security requirements of NIST SP 800-171 if awarded the contract. (If it seeks to vary from the -171 requirements, the clause allows offerors to submit requests to the DoD CIO office, for its "adjudication," but this has occurred infrequently.) The "Safeguarding" clause, 252.204-7012, appears in awarded contracts. It requires "adequate security" on "covered systems" and obligates contractors to implement SP 800-171 "as soon as practical, but not later than December 31, 2017." It also requires reporting of "cyber incidents" within 72 hours of discovery. December 31, 2017 is not a "drop dead" date. DoD does *not* require, and does *not* expect, that contractors will be in full compliance with all 110 SP 800-171 controls by December 31. DoD does expect contractors to complete a "System Security Plan" (SSP) by that date, as is discussed below. With an SSP, completion of planned security objectives can occur after Dec. 31, 2017. There is no "final date" by which all measures must be implemented; companies can take the time that they need *provided* the SSP and accompanying "plan of action" are done by Dec. 31, 2017.

3. **IMPLEMENTATION:** Many companies are unsure about what to do and whether they can act in time. Will DoD grant relief, extend the due date, or change the regulation?

There are widespread reports of contractor objections. Some prominent trade associations are pressing for delay. Nonetheless, there is little reason to expect DoD will grant relief. The rule is the product of DoD's "risk assessment," taking into account threat, vulnerability and consequence of attack. These conditions have not changed for the better since the DFARS was promulgated in Oct. 2016. Eventually, but not in the near term, the regulation may be revised to reflect experience. For the moment, however, the Administration has "frozen" new rules. An important recent development was the release, on Sep. 21, 2017, of an "Implementation Memorandum" by Shay Assad, Director of Defense Procurement and Acquisition Policy (DPAP), which should be read by every contractor. It explains that it is *DoD's* obligation to inform the contractor what is CDI, discusses how the SSP can be used to support "planned implementation" of SP 800-171 safeguards, and elaborates upon how the Government can consider a contractor's -171 implementation in the source selection process. http://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf. It also points to helpful resources to assist contractors with compliance.

4. **IMPLEMENTATION:** Why does DoD insist on the NIST SP 800-171 controls? Are other security practices adequate?

NIST developed SP 800-171 in close cooperation with NARA (the agency responsible for "Controlled Unclassified Information" rules) and DoD. It is specifically designed for use with commercial and other non-federal systems. It adopts a premise that companies should "use what they have" to achieve security, rather than mandating federal-specific methods or a federal approval process. Yet, SP 800-171 remains consistent with the security approach used for federal information systems. SP 800-171 organizes the 110 controls in 14 "families," such as Access Control ("AC"), Configuration Management ("CM"), Identification and Authentication ("IA"), Incident Response ("IR") or Security Assessment ("SA"), for example. Notably, each control is expressed in a single sentence; they are in the nature of "performance goals" rather than prescriptive "design specifications." SP 800-171 also recognizes that companies may have built their existing security using practices other than those described in NIST publications. For that reason, the -171 document contains "maps" to the international standard ISO 27001. (There also is a map to NIST SP 800-53 which compiles the many specific controls and enhancements that must be satisfied by federal agencies or companies who operate "federal information systems" on behalf of federal agencies.) In making SP 800-171 the required controls to protect CDI, DoD intends that its commercial suppliers use the 110 enumerated safeguards in SP 800-171 to check and improve security practices already in place. Nonetheless, companies also should appreciate that the DFARS seeks more than one-time "compliance;" rather, the regulation requires "adequate security in a dynamic environment." This may require companies, where indicated by assessed risk or vulnerability, to apply "other security measures." One of the required safeguards (3.12.3) requires companies to monitor security controls "on an ongoing basis" while another (3.12.4) requires periodic updates to system security plans.

5. **IMPLEMENTATION:** What is a System Security Plan (SSP) and why is it important?

SP 800-171 imposes no required format or minimum content for a SSP. Companies should approach its preparation with a risk-informed assessment which takes into account the nature and source of information they receive from or generate for the Government, the nature of their information systems, their present security measures, and the resources they can apply. In other words, each SSP is distinct to the enterprise which prepares it. A SSP should include a self-assessment. SP 800-171 calls for attention to policy and process, IT system configuration, and to hardware and software. The SSP should begin with an informed comparison of what is in place or planned, on the one hand, with each of the 110 safeguards. Where risks are found or gaps are identified, a company should document a plan to mitigate the risks and close the gaps. There is no deadline to complete the action plan. In fact, DoD recognizes that some of the more difficult -171 requirements, such as "multi-factor authentication," may not be completed until well after the Dec. 31, 2017 "compliance" date. The DPAP memorandum of Sep. 21, 2017 stresses the importance of the SSP; indeed, it is

described as a "critical input to an overall risk management decision" of whether a federal requiring activity should entrust CDI to potential contractors. Although the SSP should be documented, there is no current or generally applicable requirement for companies to disclose their SSP to any government officer, and there is no DFARS obligation that subcontractors disclose their SSP to a higher tier (prime) contractor. Companies should recognize, however, that the DCMA may check to see that a SSP was prepared, and the SSP may be scrutinized for adequacy should there be a reported cyber incident with adverse impact. Moreover, and as explained in the DPAP memo, requiring activities can request, evaluate and even score SSPs in an acquisition and competition process.

6. **IMPLEMENTATION:** Can contractors outsource compliance to other entities? What are the rules for cloud?

Third parties can provide expertise, install and maintain hardware and software, and offer independent perspective. Even so, the DFARS clearly makes the company responsible to satisfy -171 and to provide "adequate security." Some companies may consider "managed security services" or moving their Covered Defense Information to third party cloud. First, any third party given access by a company to its CDI itself must satisfy -171 and the DFARS. Second, use of cloud services, to transport, host or process CDI, is a special subject with additional requirements. DoD sees cloud as a larger target and presenting distinct security concerns, meriting higher minimum security. The DFARS -7012 clause says that cloud used by commercial companies to process or host CDI must have security "equivalent" to "FedRAMP Moderate." FedRAMP is a government-sponsored process of third party review and approval of cloud security. FedRAMP Moderate requires demonstration of security practices much more demanding than the -171 safeguards that apply to the "on-premises" systems of contractors. DoD also emphasizes that the "client" (customer) of a cloud service provider (CSP) must implement the -171 safeguards for its on-premises systems that rely upon the cloud. The client also must assure that the CSP agree to the DFARS incident reporting requirements and to cooperate with forensic measures if requested.

7. **IMPLEMENTATION:** Who in the Government can answer questions about the DFARS? Is there anyone who can review proposed practices or approve exceptions?

Companies can inform the DoD CIO's office of why a particular security requirement is not applicable, or how they are using an alternative but equally effective measure. Relatively few companies have made such submissions. Most of the 110 controls of -171 are general enough to allow a range of reasonable interpretations. Companies can "do enough" if they document their reasoning for how they interpret and apply DFARS or -171 requirements. Moreover, there are practical barriers to having compliance conversations with the Government. During an acquisition, for example, the Government's procurement team may refuse to have any discussions. Also, it may be a challenge to find Government persons who

at once are responsible for an acquisition, can speak for the risk objectives of a requiring activity, and who are informed about the DFARS rule and technically competent to comment on security practices (!). At present, DCMA oversight personnel have limited expertise, and the typical Contracting Officer cannot be expected to know much about this domain. Under the DFARS, and as explained by the DPAP Memorandum, the "requiring activity" responsible for a program is a most important actor to consider supplier cyber risk.

8. **IMPLEMENTATION:** Are there compliance reporting requirements? If so, who reviews and approves compliance? Is any "certification" required?

Neither the DFARS not SP 800-171 depend upon any third party review or certification. In fact, DoD decided neither to require nor accept third party assessment or "accreditation." When a company executes a contract with the -7012 "Safeguarding" clause, it commits to implement the -171 controls as soon as possible (but no later than Dec. 31, 2017), to provide "adequate security," and to promptly report any cyber incident. As to reporting, the regulation requires companies to have a "Medium Assurance Certificate" so they can communicate event information rapidly, and through secure means, to the DC3. Recent DoD guidance indicates that DCMA oversight personnel may check whether companies have obtained the Certificate. Filing an incident report with DC3 itself does not establish non-compliance with the DFARS and -171 requirements. However, after such a report is filed, DoD will assess the impact of the breach upon national security, and DoD may follow by asking to review the SSP even if never before submitted to the Government.

9. **APPLICATION:** What is Covered Defense Information (CDI) and how is it different from Controlled Unclassified Information (CUI)?

As defined in the DFARS, "CDI" means "unclassified controlled technical information" (CTI) *or* "other information that as described in the 'Controlled Unclassified Information' (CUI) Registry.'" The referenced Registry is maintained by the National Archives and Records Administration (NARA), which has the responsibility within the Executive Branch to coordinate protection of all types of federal information that agencies must protect by reason of law, regulations or Governmentwide policy. NARA issued the final CUI regulation on Sep. 14, 2016. At https://www.archives.gov/cui/registry/category-list, readers can find the Registry. It is not difficult for most defense contractors to identify CTI since it is technical information of military or space significance. Problems are presented by the other kind of CDI, namely CUI. As evident from the NARA Registry, CUI embraces all 23 categories and 84 subcategories of information that federal agencies must protect. Many companies possess information of a type that could be categorized as CUI. (Often, separate statutes or regulations apply to such information.) But this does not mean that all information that is conceivably CUI must be protected per the DFARS and in accordance with SP 800-171. My analysis is that the DFARS does *not* apply unless the information in question (a) meets a Registry definition of CUI, (b) was *provided* by the Government to a

contractor *and* (c) was *designated* as CUI by the Government. The purpose of the DFARS is to not to protect all information in the possession of a contractor but *Government* information, as defined. CUI can be provided by the Government to the contractor, or delivered by the contractor to the Government, but in either case the DFARS should apply only to that information which DoD has marked or otherwise identified. It may be "prudent" for companies to protect other information, such as employee records, or unmarked technical data, but this is *not* a DFARS requirement absent Government designation and direction, or special contract requirement.

10. **APPLICATION:** Who is responsible for the identification of CDI or CUI in a contract?

Here, the specific language of the Sep. 21 DPAP Memorandum is key. It states:

> "The Department must mark, or otherwise identify in the contract, any covered defense information that is provided to the contractor, and must ensure that the contract includes the requirements for the contractor to mark covered defense information developed in the performance of the contract."

(Emphasis added.) In the -7012 clause itself, the definition of "Covered Defense Information" is not a model of clarity. First it says that CDI "is marked or otherwise identified" in the contract *and* "provided to the contractor by or on behalf of DoD." But the clause goes on to include, also, information that is "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor *in support of* the performance the contract." (Emphasis added.) The last part of the definition has caused a lot of confusion. What is meant by "in support of" performance? Is the data used in a company's payroll system considered "in support of performance," and therefore CDI? The recent DPAP Memorandum answers most variations of this question. It is the Government's responsibility to inform the contractor what is CDI if it is provided by the Government to the contractor. The regulation also protects information that the Government pays the contractor to create and to deliver to the Government. There too, the Government must inform the contractor what information is to be protected. (To note, some requiring activities take a different and more expansive view; if so, they must inform the contractor in the solicitation and by the contract.)

This concludes Part I of "The Cyber DFARS: Key Questions, Asked & Answered." Part II continues the analysis with ten additional questions and answers. Subjects to be addressed in Part II include whether SP 800-171 applies to information accumulated by a contractor before award of a contract subject to the -7102 DFARS; problems and responses that arise in dealing with the supply chain; issues that arise with small business and commercial suppliers; how cyber compliance can figure into eligibility for contract award and in competitive evaluation; details of the cyber reporting obligation; how the Government may

enforce the obligations; and what to expect in the future from DoD and the civilian federal agencies.

Hopefully, this document responds to your concerns about interpretation, application and implementation of the cyber safeguards required by the DFARS and SP 800-171. Should you have more questions, contact Bob Metzger at rsm@rjo.com or (202) 777-8951.

> This document may be subsequently modified or supplemented. It is a copyrighted expression of the author's analysis and should not be quoted, excerpted, copied or otherwise used without full acknowledgement.

---

[i] This article expresses the personal views of the author and should not be attributed to the Department of Defense, the Defense Science Board, to any other organization with which he is involved or may be affiliated, or to any client of Mr. Metzger or of Rogers Joseph O'Donnell, PC.