dentons.com

DENTONS

Insights and Commentary from Dentons

The combination of Dentons US and McKenna Long & Aldridge offers our clients access to 1,100 lawyers and professionals in 21 US locations. Clients inside the US benefit from unrivaled access to markets around the world, and international clients benefit from increased strength and reach across the US.

This document was authored by representatives of McKenna Long & Aldridge prior to our combination's launch and continues to be offered to provide our clients with the information they need to do business in an increasingly complex, interconnected and competitive marketplace.

Bloomberg BNA

Federal Contracts Report™

Cybersecurity

Don't Be an Example; Why Focusing Now on the Recent DFARS UCTI Rule is Essential




BY ELIZABETH A. FERRELL, PHILLIP R. SECKMAN, ERIN B. SHEPPARD, MICHAEL J. MCGUINN

The NIST Cybersecurity Framework and the General Services Administration/Department of Defense effort to incorporate cybersecurity standards into federal acquisitions have captured headlines in recent months. These government initiatives—at least for now—do not impose any mandatory obligations on government contractors. With significantly less fanfare, DOD since November 18, 2013 has included a clause in new contracts that does, presently, impose *mandatory* security controls and reporting obligations on *all* DOD prime contractors and subcontractors handling ''unclassified controlled technical information'' (UCTI). Many DOD contractors and subcontractors, particularly in the supply chain, remain largely unaware of the significant compliance implications of this new contract clause, DFARS 252.204-7012.

Elizabeth Ferrell (eferrell@mckennalong.com) and Phillip R. Seckman (pseckman@mckennalong.com) are partners in McKenna Long & Aldridge LLP's government contracts practice. Erin B. Sheppard (esheppard@mckennalong.com) and Michael J. McGuinn (mjmcguinn@mckennalong.com) are associates in the firm's government contracts practice.

This third article in the Federal Contracts Report's series on cybersecurity provides practical guidance and key takeaways for government contractors seeking to comply with the requirements of the DFARS UCTI clause. Specifically, we address the following issues: (1) applicability of the DFARS clause and its requirements; (2) implementation of the clause's security controls; (3) the clause's reporting requirements; (4) supply chain implications; and (5) cost recovery of compliance efforts.

DFARS Clause Applicability. The new DFARS Clause will be located in Section I of *any* DOD funded government prime contract awarded after November 18, 2013. If performing a subcontract, the clause is likely to be included in an attachment or exhibit to the subcontract (e.g., in standard terms and conditions). It will be located along with other FAR and DFARS clauses that the higher-tier contractor is seeking to flow down to the subcontractor.

The DFARS clause is mandatory in DOD funded contracts awarded after November 18, 2013, without exception, and regardless of dollar value, procurement method (*i.e.*, commercial items, simplified procurement, etc.), or size status of the awardee. DFARS 204.7303. Additionally, the substance of the new DFARS clause (including the clause's flow down requirement) must be included in all subcontracts (regardless of tier), including subcontracts for commercial items. DFARS 252.204-7012(g). This presents supply chain implications that will be discussed further below.

 ISSN 0014-9063

Practice Tips

— Check section I of prime contracts or the relevant appendix/exhibit of subcontracts to determine if DFARS 252.204-7012 is included.

— If subject to the DFARS clause, take prompt action to implement the mandated security controls.

— Maintain robust documentation supporting compliance with the DFARS information system security controls.

— Prime contractors: report subcontractor cyber incidents to the DOD. Subcontractors: ensure proprietary information disclosed in connection with an investigation is protected.

Provided the DFARS clause is included in a contract, a contractor or subcontractor should carefully determine whether the substantive requirements of the clause are applicable. The safeguarding and reporting requirements of the clause only apply when a contractor has or will have UCTI resident on or transiting through its unclassified information systems. It is therefore critical that responsible contractor personnel understand precisely what qualifies as UCTI.

Unfortunately, the definition of UCTI under the DFARS clause is not as simple as one might hope or expect. The DFARS clause defines the term ''controlled technical information'' as follows:

technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with DOD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

DFARS 252.204-7012(a). ''Controlled technical information,'' therefore, has three elements: (1) technical information; (2) with military or space application; and (3) that is to be marked in accordance with DOD Instruction 5230.24. ''Technical information'' means technical data or computer software, as those terms are defined in the clause at DFARS 252.227–7013, Rights in Technical Data—Non Commercial Items. This technical information also must have a ''military or space application'' to be subject to the rule, a test that likely will have broad applicability.

The third element, the UCTI marking requirement, creates ambiguity for contractors. Although an argument exists that the rule only applies to technical information that has been marked pursuant to DOD Instruction 5230.24, the UCTI definition also includes technical information that ''is to be marked.'' *See* DFARS 252.204-7012(a). Contractors should understand, therefore, that the responsibility to safeguard covered data may exist even if it has not yet been marked. For example, in the course of contract performance, contractors may develop data that, upon delivery to DOD, will be marked in accordance with the specified DOD Instruction. Likewise, contracting officers may also direct contractors to mark data based on the DOD instruction. The potential need for safeguarding of data not yet marked highlights the need to train contractor personnel to ensure that there is a full understanding and ability within the relevant company functional areas to identify documents and other information that is to be marked, but that has not yet been marked.

The key takeaways on the applicability of the DFARS UCTI clause include:

- Contractors should check Section I of prime contracts or the relevant appendix/exhibit of subcontracts to determine if DFARS 252.204-7012 is included.

- Contractors should consider submitting a bidder's question asking the government whether the contract will involve UCTI. Although the government could potentially change its position at a later date, the government's response will help contractors avoid future UCTI surprises and bring systems into compliance with the clause before award, as appropriate.

- Contractors should train responsible personnel on how to identify UCTI and consider developing a company policy or procedure to aid responsible personnel in making the determination.

Security Controls Implementation. If the DFARS clause has already been included in contracts or subcontracts and government contractors have UCTI resident on or transiting through their information systems, contractors should promptly take appropriate steps to ensure compliance with the clause. This includes the implementation of more than 50 security controls, or their equivalent, required by the clause. If a contractor's current information system security controls do not achieve the standards specified in the applicable criteria in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, or their equivalent, then the contractor must immediately undertake efforts to implement a plan to achieve compliance or notify the Contracting Officer or prime contractor that a required security control is not applicable. *See* DFARS 252.204-7012(b)(1)(ii).

The DFARS clause provides that the contractor and its information systems security program ''shall implement'' the enumerated NIST security controls. DFARS 252.204-7012(b). This language arguably suggests that a contractor has a period of time to accomplish implementation of the required information system security controls; however, any potential implementation period is not open-ended. A contractor's failure to undertake prompt action and demonstrate concrete progress invites DOD (or any higher-tier contractors) to argue that such foot-dragging amounts to breach of contract. As discussed in more detail below, a contractor may also demonstrate compliance through use of equivalent security controls. Whether through the enumerated controls or their equivalent, contractors must move swiftly to implement such controls.

In addition to the issue of *when* implementation must occur is the question of *how* it should occur, and specifically, whether certain controls should be prioritized over others. Although not directly included in the DFARS clause, NIST SP 800-53 contains guidance for contractors on security control prioritization that likely will be considered reasonable guidance for implementation. NIST SP 800-53 assigns each of the controls within that publication, including the controls identified and incorporated into the DFARS rule, a prioritization code designation. Organizations can use this designation ''to as-

  FCR ISSN 0014-9063

sist in making sequencing decisions for control implementation.'' *See* NIST SP 800-53 at 12. A Priority Code 1 (P1) control has a higher priority for implementation than a Priority Code 2 (P2) control, and a P2 control has a higher priority for implementation than a Priority Code 3 (P3). *Id*.

Many of the DFARS controls are P1 priority. Absent any definitive guidance in this area, contractors and subcontractors likely have some reasonable discretion to prioritize the implementation of security controls with the same prioritization code. In reality, however, any implementation approach taken likely will be subject to challenge from DOD in the event of a breach, as DOD will have the benefit of hindsight and will argue that a contractor or subcontractor should have been fully compliant with the NIST controls when it received its first contract containing the DFARS clause. While such a conclusion is arguably unreasonable, it presents a risk and an incentive for contractors to proceed expeditiously to implement the security controls that the DFARS clause requires, regardless of the control's prioritization level.

Once a contractor concludes that the DFARS clause is applicable and the contractor develops an implementation plan with appropriate prioritization of security controls, the next step is to identify the controls that must be implemented. The DFARS clause, in Table 1, specifies the ''minimum security controls for [UCTI].'' The Table, however, in some cases lists a control enhancement (e.g., AC-17(2) but *not* the related baseline control. For example, Table 1 within the DFARS clause specifies AC-3(4) — Discretionary Access Control, but does not expressly specify that the baseline control AC-3 – Access Enforcement must also be implemented. This prompts the obvious question: Do contractors need to implement the baseline control too?

Consistent with well-established principles of regulatory construction, one might be tempted to conclude that the plain language does not include the baseline and, therefore, it is inapplicable. Table 1 provides, however, that ''[a] description of the security controls is in the NIST SP 800-53.'' Thus, proper implementation of the DFARS clause security controls arguably also requires an understanding of NIST SP 800-53 and related documents to determine whether those publications contemplate that an enhancement can be implemented independently of the related baseline control.

NIST SP 800-53 explains the relationship between control enhancements and related enhancements. Specifically, the document provides that ''[c]ontrol enhancements are not intended to be selected independently (i.e., if a control enhancement is selected, then the corresponding base security control must also be selected).'' The bottom line is that, in the event of a cyber incident, DOD likely will look for and expect compliance with the baseline control when an enhancement is specified. Accordingly, contractors should carefully consider ensuring the baseline controls are satisfied even though they are not specified in the clause.[1]

Importantly, a contractor or subcontractor is not necessarily required to implement any baseline control or associated control enhancement if the contractor can provide the Contracting Officer or prime contractor with a written explanation of how the required control is not applicable or how an alternate existing control or protective measure is used to achieve equivalent protection. This exception is critical for contractors who have based their control programs on alternate standards. Though determining equivalence will still require a firm understanding of the NIST SP 800-53 requirements, this exception provides a crucial alternative method for demonstrating compliance.

Finally, although the clause requires the contractor to advise the Contracting Officer if NIST controls are inapplicable or equivalent protections are being used, the clause does not contemplate or require contractors to obtain either system approval or an adequacy determination for its security systems. This is potentially good for contractors, in that it does not impose the administrative burdens associated with such approvals. And, there is no reason to believe that a DOD Contracting Officer would have the technical competence to assess whether, in fact, a contractor's adopted safeguards and information security policies and practices actually comply with the NIST control criteria. The current DFARS rule imposes requirements on contractors, but compliance will likely be evaluated only with the benefit of 20/20 hindsight through the trials and errors of contractors who suffer a breach. As such, even though no government approval is required, the stakes for contractors are high.

For the time being, contractors should document how the entity itself has determined compliance and keep a record of that determination on file so that it is available in the event of a reportable cyber incident or other audit. Such documentation will likely be critical in the face of a reportable incident.

The key takeaways concerning implementation of the DFARS clause include:

- Contractors and subcontractors that are subject to the DFARS clause must take prompt action to implement the mandated security controls. As time passes since the final rule was promulgated, the risk that a contractor may be found noncompliant will likely increase.

- As part of the implementation plan, contractors should consider prioritizing controls in a manner that is consistent with NIST SP 800-53 and the contractor's particular circumstances.

- Particularly for lower-tier subcontractors, contracts and sales personnel should be trained to be wary of executing certifications or representations of compliance as doing so creates the potential risk of later misrepresentation claims if a cyber incident occurs and your information system security controls are determined non-compliant, particularly in the event of a breach.

- In addition to implementing the specified NIST controls, contractors must consider whether other controls are necessary (and, if not, documenting the reasons for this conclusion).

- Contractors should be mindful of the risk that failure to implement certain baseline security controls, even though they are not expressly specified in the DFARS clause, could result in the contractor being found non-compliant.

- Contractors should consider the option of notifying the contracting officer or prime contractor that a

[1] These baseline controls associated with enhancements specified in Table 1 are: (1) AC-3; (2) AC-11; (3) AC-17; (4) AC-18; (5) AC-20; (6) AU-6; (7) IA-5; (8) SC-8; and (9) MA4.

NIST security control is not required because the contractor has an alternative control or protection that achieves equivalent protection. Even though approval is not required, in the event the contracting officer or prime concurs, such determination or agreement should be memorialized in writing.

■ Contractors should carefully document the methodology employed when establishing their information security systems as well as the basis for their determination that their information security systems are compliant with the DFARS clause.

The DFARS Clause Reporting Requirements. Subparagraph (d) of the DFARS clause specifies detailed reporting requirements for cyber incident and data compromises. DFARS 252.204-7012(d). The heart of the requirement is that a prime contractor must provide a report to DOD within 72 hours of a ''cyber incident.'' A ''reportable cyber incident'' includes ''[a] cyber incident involving possible exfiltration, manipulation, or other loss or compromise of *any [UCTI]* resident on or transiting through Contractor's, or its subcontractors', unclassified information system'' and ''[a]ny other activities. . . that allow unauthorized access to the Contractor's unclassified information system which has [UCTI] resident on or transiting.'' DFARS 252.204-7012(d)(2).

The contractor's cyber incident report must contain certain categories of information, if possible, including: (i) affected contract numbers unless all contracts by the company are affected; (ii) name of the subcontractor and CAGE code if this was an incident on a subcontractor network; (iii) DOD programs, platforms or systems involved; (iv) location(s) of compromise; (v) date incident discovered; (vi) the type of compromise (e.g., unauthorized access, inadvertent release, other); and (vii) a description of the technical information compromised.

In addition to these initial reporting requirements, contractors experiencing such an event must also conduct a further review of the affected networks for evidence of compromise resulting from a cyber incident to include, but not limited to, ''identifying compromised computers, servers, specific data and users accounts.'' DFARS 252.204-7012(d)(4). Additionally, the contractor must review the data accessed to identify the specific UCTI implicated in the incident and take the necessary forensic steps to preserve and protect images of known affected information systems and all relevant monitoring/packet capture data for at least 90 days from the cyber incident to allow DOD time to request the information.

Importantly, a contractor's reporting obligation exists separately from its obligation to implement the NIST security controls in the clause. This means that contractors currently considering how to implement the clause's security controls must still comply with the clause's reporting requirements even if such a program is not yet in place. Certainly, one interpretation of the clause is that a contractor in the process of implementing the DFARS security controls must self-report a cyber incident that could, in turn, highlight the contractor's failure to implement compliant security controls. The reporting obligation, and the foregoing risk, should further encourage contractors to promptly implement the required security controls.

The key takeaways concerning the DFARS reporting requirement include:

■ Contractors should maintain robust documentation supporting the contractor's compliance with the DFARS information system security controls to counter any DOD contention to the contrary in the event of a cyber incident.

■ Contractors should establish reporting processes that identify the required information and steps necessary to respond to and report a cyber incident. Given the 72-hour reporting requirement, these details and specific methodology should be addressed and documented with specificity before an incident so that the response team can focus immediately on data collection.

■ In addition to creating a detailed, written incident response plan, contractors should consider establishing a team that is ''on-call'' to rapidly respond to any reportable incident.

■ Prime contractors are responsible for reporting subcontract incidents to DOD. Prime contractors must therefore ensure that any DOD subcontracts require subcontractors to report the DFARS-required information to the prime contractor. DFARS 252.204-7012(d)(1) should be appropriately modified to reflect the fact that subcontract reports must be to the prime contractor sufficiently in advance of the 72-hour reporting deadline.

■ Information required by the rule must be appropriately preserved and back-up systems must be in place to protect the company's interests. A contractor's incident response plan should outline the specific steps required to preserve and back-up any such information in the event of a breach.

Supply Chain Considerations. The new DFARS clause includes a requirement that all prime contractors and subcontractors include the substance of the DFARS clause as a mandatory flowdown in all subcontracts. The government has recognized the interrelated nature of the modern supply chain and the fact that adversaries seeking to exfiltrate information from a target may obtain access to that target's data by means of exploiting the information system of its suppliers. To address this issue and in an effort to impose greater security and rigor throughout the supply chain, the DFARS clause is a mandatory flowdown regardless of the subcontract dollar value, subcontract type, or size status of the subcontractor.

A different, but critical issue, that we noted in the preceding section is that the reporting requirements of the DFARS clause contemplate that one of the items that a prime contractor is to report is the ''name of subcontractor and CAGE code if this was an incident on a subcontractor network.'' In other words, the DFARS clause appears to contemplate that a cyber incident that occurs deeper in the supply chain is to be reported along the chain of privity and ultimately to the government through the prime contractor. Additionally, a prime contractor may attempt to structure its flowdown clause to give it a right of access to subcontractor networks to make sure that the subcontractor is accurately identifying compromised UCTI and reporting it up the chain.

Any subcontractor dealing with a competitor company likely will be less than enthused at the prospect that: (1) any cyber incident must be reported to the competitor prime contractor; or (2) the prime contrac-

  FCR ISSN 0014-9063

tor may attempt to include in the subcontract the ability to seek access to and/or information from the subcontractor's data systems that could potentially compromise trade secrets or other competition and/or business sensitive information. Indeed, real risk exists that, where UCTI and confidential business information reside on the same subcontractor network, investigation of compromised UCTI could result in the compromise and exposure of the subcontractor's proprietary pricing and other contract intelligence and supply management capabilities to its competitor prime or higher-tier subcontractor.

Subcontractors faced with a prime contractor's attempt to gain access to information systems should proactively address the business risk that other aspects of their proprietary systems may be revealed and/or subject to review as part of a cyber incident investigation and take steps to ensure that any such incident investigation is narrowly focused on the affected systems (as opposed to aimed at accessing any competitively sensitive information). Subcontractors may want to consider crafting a non-disclosure agreement that anticipates and reasonably addresses these concerns and seeks to ensure that any prime contractor review team will be considered a ''Clean Team'' that accesses and reviews information solely for purposes of satisfying the substantive requirements of the DFARS clause that are flowed down.

Another potential concern that arises in this supply chain context is the lack of a mechanism to seek or obtain approval of information system security compliance with the DFARS clause requirements. Just as prime contractors will not have their systems reviewed or approved by a contracting officer, subcontractors will not receive any affirmative approval or recognition that their information system security controls are compliant. Instead, compliance likely will be determined in the aftermath of a cyber breach. Thus, it will be just as important for subcontractors to document compliance as it is for prime contractors. At a minimum, even if the company's cybersecurity protections are later challenged as being noncompliant, evidence of the efforts undertaken to achieve compliance are likely to help tip the scales to ensure that any liability remains purely contractual and does not create risk of other adverse agency or government action. Subcontractors, like prime contractors, should contemporaneously document internally their compliance using the NIST controls or equivalent protections.

Given the depth to which this clause will flow down into the DOD supply chain, it is inevitable that the requirements of the clause will have a disproportionately significant impact on medium and small government contractor companies. Larger defense contractors are much more likely to have already in place information system security controls that are largely compliant with the NIST SP 800-53 or equivalent controls that the DFARS clause requires. By contrast, smaller firms are more likely to utilize third-party vendors to support their business operations. Critically, the DFARS clause specifically contemplates that these third-party service providers are to be considered subcontractors. *See* 78 Fed. Reg. 69273 (Nov. 18, 2013) (stating that ISPs and cloud service providers are subcontractors subject to the DFARS clause). Although significantly different in certain respects, ISPs and cloud service providers both transmit and/or store data on behalf of users. Another service that may be used by contractors are email service providers like Google, Yahoo, and AOL that serve similar functions. As a result, one interpretation of the DFARS clause is that it would treat all third-party service providers, including email service providers, ISPs and cloud service providers, like subcontractors.

Of course, this completely ignores the business reality and significant lack of negotiation leverage that can be exercised to induce ISPs and other providers to accept the DFARS clause. Thus, small businesses that are contractually obligated to comply with the flowdown obligation may find themselves between a rock and a hard place as to what to do in the face of this new reality.

Notably, the NIST controls recognize that organizations will have different levels of trust in external service providers. ''For example, separately authorized external information system services provided to organizations through well-established lines of business relationships may provide degrees of trust in such services within the tolerable risk range of the authorizing officials and organizations using the services.'' NIST SP 800-53 at 19; *see also* NIST SP 800-39, Managing Information Security Risk (describing different trust models that may be employed by organizations when establishing relationships with external service providers). NIST recognizes that in certain cases ''when organizations are not in a position to require explicit agreements with external service providers (e.g., services are imposed on organizations, services are commodity services), organizations establish and document explicit assumptions about service capabilities with regard to security.'' NIST SP 800-53 at 19. In contrast to NIST, the DFARS clause treats all subcontractors and suppliers the same without considering the level of trust in various suppliers. But when a contractor or subcontractor is unable to get its ISP or cloud service provider to enter into an agreement containing the DFARS clause, NIST SP 800-53 suggests that the next best alternative is to establish and document the ISP or cloud service provider's security capabilities, and to establish a history of trustworthiness with the provider.[2]

The key supply chain takeaways include:

- Prime contractors are responsible for reporting subcontractor cyber incidents to DOD. Subcontractors should take steps to ensure that proprietary information disclosed in response to or during an investigation of a cyber incident, if any, is protected. This may include limiting access to an incident response team.

- Subcontractors should assess and document compliance with DFARS security controls in the same manner as prime contractors.

- ISPs and other external service providers will likely be unwilling to accept flowdown requirements. Contractors faced with this refusal should: (1) ensure they obtain the provider's refusal in writing; (2) consider minimizing the use of these external service providers if at all possible; or (3) establish and document the ISP or external service provider's security capabilities, if known, and any other factors showing the pro-

[2] Of course, the NIST alternative just discussed lacks the reporting requirements that the DFARS clause imposes, and there likely will be little contractors can do to require these external providers to report such information.

vider's trustworthiness (e.g., historical relationship with provider, known breach history).

Cost Recovery. The portion of the DFARS rule that addresses comments received during the notice and comment period states that reasonable costs of complying with the DFARS clause should be allowable. Importantly, the preamble goes on to specify that such costs are, generally, chargeable as indirect costs. *See* 78 Fed. Reg. at 69275 (''In many cases, this contract requirement will be spread across and benefiting multiple contracts—costs associated with implementation will be allowable and chargeable to indirect cost pools.''). Importantly, if a contractor is awarded a single contract that creates the obligation to implement the information system security controls required by the rule, or if the contractor can establish that the casual beneficial relationship indicates that allocation of the implementation costs as indirect would be inequitable, then the contractor should consider identifying the costs as direct or utilizing special allocation basis. The mere statement in the DFARS preamble that the costs are to be generally treated as indirect costs certainly does not require that treatment in all circumstances. Instead, contractors should assess proper allocation of the cost as direct or indirect in accordance with their established practices.

Summary. As detailed above, the new DFARS clause regarding UCTI creates significant near and long term compliance requirements for government contractors. The burden of these requirements, in the near term, are expected to fall disproportionately on medium to small-sized government contractors as well as commercial companies that happen to be providing supplies or services that ultimately support a government prime contract. Additionally, we anticipate that other reporting requirements – for example those announced in Section 941 of the 2013 NDAA –will soon be implemented in government regulations. Thus, the DFARS rule on safeguarding and reporting relating to UCTI is truly a precursor to future cybersecurity developments coming down the road.

  FCR ISSN 0014-9063