Government Contracts Advisory

JULY 5, 2011

CONTACTS

For further information regarding the topic discussed in this update, please contact one of the professionals below, or the attorney or public policy advisor with whom you regularly work.

Elizabeth A. Ferrell
202.496.7544

Erin B. Sheppard
202.496.7533

Proposed DFARS Rule Mandates New Security, Monitoring, and Reporting Obligations to Protect DoD Information on Unclassified Contractor Information Systems

On June 29, 2011, the Department of Defense ("DoD") issued a Proposed Defense Federal Acquisition Regulation Supplement ("DFARS") Rule establishing basic safeguarding requirements applicable to non-public DoD information residing on contractor non-classified information systems, and imposing heightened safeguarding requirements and incident reporting obligations for certain categories of information. **76 Fed. Reg. 38089** (June 29, 2011). The Proposed Rule imposes substantial compliance obligations for protection of unclassified information. Contractors and subcontractors who currently have or may potentially have unclassified DoD information resident on or transiting through their unclassified information systems should familiarize themselves with the proposed restrictions and should consider submitting comments on the Proposed Rule. Comments are due by August 29, 2011.

The Proposed Rule adds a new subpart, DFARS 204.74, containing a policy statement, procedures, and corresponding contract clauses. The Proposed Rule applies to nonpublic DoD information (1) that has not been cleared for public release and (2) provided by or on behalf of DoD or collected, developed, received, or transmitted in conjunction with the contractor's support of an official DoD activity. The Proposed Rule revises the existing contract clause governing disclosure of nonpublic DoD information, DFARS 252.204-7000, and imposes affirmative obligations on contractors and subcontractors for the protection of such information residing in or transiting through contractor information systems. Under the Rule, Contracting Officers ("CO") must obtain guidance from the requirements office to determine which level of protections should apply to a particular contract. 76 Fed. Reg. at 38092.

DoD previously published an Advance Notice of Proposed Rulemaking ("ANPR") and Notice of Public Meeting in March 2010 to provide the public an opportunity in the rulemaking process. See 75 Fed. Reg. 9563 (Mar. 3, 2010). A public meeting was held on April 22, 2010.

The Proposed Rule includes some changes to help clarify the rule's applicability and remove some of the discretion potentially afforded to Contracting Officers, but largely fails to address some of the larger

concerns raised by commenters on the ANPR. For example, the Proposed Rule continues to rely upon DoD Directives and internal DoD documents to define the categories of information subject to Enhanced Safeguarding Requirements. Some industry and trade groups had warned that the reliance on such DoD instructions made it inherently difficult for contractors to assess the applicability of the Proposed Rule. Similarly, the Proposed Rule does not address criticisms from industry that recommended waiting until the National Archives and Records Administration ("NARA") has completed its review of controlled unclassified information prior to issuing such guidance. Rather than wait for the completion of that streamlining process, DoD simply notes that the rule will be subject to revision based on NARA's ongoing efforts. Finally, the Proposed Rule does not address concerns regarding the breadth of the rule's application to commercial item contracts, small businesses, and down-stream suppliers.

The Proposed Rule establishes two levels of safeguards: Basic and Enhanced. The Basic requirements apply where the DoD requiring activity determines that the contractor or a subcontractor will potentially have DoD information in its unclassified information systems. 76 Fed. Reg. at 38092 (DFARS 204.7404). In such circumstances, the CO shall include a new DFARs clause — DFARS 252.204-70XX, Basic Safeguarding of Unclassified DOD Information — in the resulting contract. The Basic Safeguarding clause requires the provision of "adequate security to safeguard unclassified government information" and defines "adequate security" as protective measures commensurate with the risks of loss, misuse, or unauthorized access to or modification of the information.

Specifically, the Basic Safeguarding clause mandates the use of seven basic safeguarding requirements: (1) requiring access control for any unclassified information posted to webpages; (2) providing security and privacy protections for e-mails, texts, and similar communications; (3) obtaining reasonable assurances for transmission of voice and fax information; (4) protecting information by at least one physical or electronic barrier when not in use; (5) sanitizing electronic media that have been used to store unclassified information before disposal or dissemination; (6) providing intrusion protections for computers and computer systems (such as malware protections and security-level software upgrades); (7) and limiting contractor and subcontractor access to information to those who have a need to know and employ such protections. Contractors must also include these requirements in any subcontract in which the subcontractor may have such information resident or transiting on its information systems. Id. at 38093 (DFARS 252.204-70XX(b)).

Under the Enhanced Safeguarding clause — DFARS 252.204-70YY, Enhanced Safeguarding of Unclassified DoD Information — contractors must comply with each of the requirements of the Basic Safeguarding clause, as well as additional, heightened safeguarding obligations. Contracting Officers must include the Enhanced clause where contractor or subcontractor will have information in one or more of the following categories:

- Information designated as critical program information in accordance with DoD Instruction 5200.39, Critical Program Information Protection;

- Information designated as critical information in accordance with DoD Directive 5205.02, DoD Operations Security Program;

- Information subject to export controls under International Traffic in Arms Regulations and Export Administration Regulations;

- Information exempt from mandatory public disclosure under DoD Freedom of Information Act Programs (DoD Directive 5400.07);

- Information bearing current or prior controlled access designations (e.g., FOUO, Sensitive but Unclassified, Limited Distribution, Proprietary, etc);

- Technical data, computer software, or other data covered by DoD Directive 5230.24, Distribution Statements on Technical Documents; and

- Personally identifiable information (to include Privacy Act and Health Insurance Portability and Accountability Act information).

The Proposed Rule lacks any further guidance on how Contractors should assess the applicability of these internal DoD Directives.

The Enhanced Safeguarding clause imposes two additional requirements on contractors with information in one or more of these categories. First, the contractor must implement an information security program in its project, enterprise, or company-wide unclassified information technology system (as applicable). Contractors must employ the specified National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53 minimum security controls. Specifically, contractors must comply with access control, awareness and training, contingency planning, maintenance, and system and communication protection standards. In the event that a contractor either considers a control to be inapplicable or proposes an alternate protective measure, such a determination should be made in writing and be made available to the Contracting Officer upon request. Contractors must also utilize only DoD-approved identity authentication credentials for authentication to DoD information systems. 76 Fed. Reg. at 38093.

Second, the contractor must comply with cyber-incident reporting and associated information sharing requirements. A contractor subject to the Enhanced Safeguarding requirements must report (1) all cyber incidents involving exfiltration, manipulation, loss, or compromise of DoD information resident in its information systems and (2) any unauthorized access to such information systems within 72 hours of discovering such an incident. Reports shall be made via a yet-to-be-created DoD website, and the contractor shall conduct a review of the incident, preserve relevant data, cooperate with DoD's Damage Management Assessment Office (and any follow-up DoD assessment), and provide necessary contacts. Contractors must mark any attribution information included in the information reported

or otherwise provided to the government. Id. at 38093-94. The Proposed Rule places strict limitations on DoD's authorization to disclose cyber-incident report information and requires the use of confidentiality requirements before disclosing any attribution information. However, where contractors must disclose third party data in order to comply with the incident reporting requirements and the data is protected by a non-disclosure provision, the contractor must either seek written permission that the information may be shared with the government or bear the risk that the third party may have the right to pursue legal action against the contractor. Id. at 38095.

As with the Basic Safeguarding requirements, the Enhanced Safeguarding clause also requires contractors to include the substance of the clause in all subcontracts that may have unclassified DoD information requiring enhanced protection. Subcontractors must report cyber-incidents to both the prime contractor and DoD.

Notably, the Enhanced Safeguarding requirements are in addition to and not in lieu of other information security requirements. The requirements do not relieve contractors of their obligations under other DoD Safeguarding requirements for certain categories of information nor do they replace any other applicable incident reporting requirements under other legislative or regulatory programs.

Although it is difficult to predict when the Proposed Rule might go into effect, there are actions contractors can take now. Many government contractors have existing internal information technology and information security policies and procedures governing the protection of government information resident on contractor information systems, and the Proposed Rule elevates those voluntary measures to a contractual compliance requirement. Contractors should therefore begin familiarizing themselves with the proposed requirements and engaging in a dialogue with DoD on the impact of these requirements. Specifically, DoD contractors should:

- **Evaluate, based on current programmatic responsibilities, whether any existing contracts will be subject to enhanced safeguarding requirements.** The Proposed Rule is silent on whether these requirements will be added by contract modification to existing contracts. However, contractors on existing programs should consider working closely with the DoD Contracting Officers to better understand the potential application of the Rule to their program(s).

- **Become familiar with the seven basic safeguarding requirements and consider drafting policies and procedures for complying with those requirements as necessary.** The minimal changes between the ANPR and the Proposed Rule suggest that these requirements will likely be included in any Final Rule. Accordingly, DoD contractors should review these requirements, including the fact that all of these requirements must be flowed down to subcontractors, and consider developing policies and procedures for compliance with these provisions.

- **Review existing subcontracts.** Contractors should assess the impact of the Proposed Rule on existing or contemplated subcontracts.

- **Engage in dialogue between Industry, DoD, and other agencies.** As drafted, it remains unclear how DoD will view cyber-incident reports when assessing contractor performance. The Proposed DFARS 204.7402 provides that a properly reported incident shall not, by itself, be interpreted as evidence that the contractor has failed to provide adequate safeguards in compliance with the clause. However, because cyber security is a dynamic and evolving area, contractors should remain closely engaged with DoD in determining how such information will be used.

- **Consider submitting comments/supporting trade group comments on the Proposed Rule.** Contractors have until August 29, 2011 to submit Comments on the Proposed rule.

McKenna Long & Aldridge will continue monitoring key developments in each of these areas and provide periodic updates.