COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Government Contracts

July 6, 2011

PROPOSED RULE WOULD REQUIRE CONTRACTORS TO PROTECT UNCLASSIFIED DOD INFORMATION

On June 29, 2011, the Department of Defense ("DoD") issued a proposed rule that would amend the Defense Federal Acquisition Regulation Supplement ("DFARS") to add requirements for protecting unclassified DoD information, and to address the risk of controlled unclassified information being accessed through cyber intrusions. This DFARS-related proposal to address and manage cyber security risk had been rumored for some time and fits within DoD's and the federal Government's broader efforts to mitigate and address cyber threats. At the same time, it would impose substantial new requirements on many contractors to safeguard unclassified DoD information within their information systems from unauthorized access and disclosure, and to report to DoD certain cyber intrusion events that affect DoD information on, or transiting through, contractor unclassified information systems.

Previously, DoD had issued broader guidance on safeguarding unclassified DoD information. In addition, through its administration of the National Industrial Security Program Operating Manual ("NISPOM"), which regulates access to classified information, DoD has implemented requirements for companies with facility clearances that operate under certain forms of foreign ownership, control or influence ("FOCI") to implement information security policies and procedures to prevent the unauthorized disclosure of classified and certain controlled unclassified information. However, neither the DFARS nor the NISPOM currently addresses safeguarding or cyber intrusion reporting requirements of security-cleared companies that do not operate under FOCI or Government contractors that do not have a facility security clearance. Thus, the proposed rule is significant because it would formalize and extend safeguarding requirements for unclassified DoD information to all Government contractors, and the proposed requirements, if implemented, could generate new compliance obligations and related costs for contractors that have DoD information on their information systems.

THE PROPOSED RULE

The proposed rule would apply to contracts when the contractor or a subcontractor at any tier will potentially have unclassified DoD information residing on or transiting through its unclassified information systems. The rule addresses the safeguarding requirements specified in Executive Order 13556, Controlled Unclassified Information, and the rule's purpose is to implement adequate security requirements to protect unclassified DoD information in contractor information systems, and to require contractors to report certain cyber intrusion events that impact unclassified DoD information. The proposed rule includes basic safeguarding requirements that would apply to any unclassified DoD information, as well as enhanced safeguarding requirements, including cyber incident reporting, that would apply to information that is:

- Designated as Critical Program Information in accordance with DoD Instruction 5200.39, Critical Program Information ("CPI") Protection Within the Department of Defense;

- Designated as critical information in accordance with DoD Directive 5205.02, DoD Operations Security ("OPSEC") Program;
- Subject to export controls under the International Traffic in Arms Regulations ("ITAR") and Export Administration Regulations ("EAR");
- Exempt from mandatory public disclosure under DoD Directive 5400.07, DoD Freedom of Information Act Program, and DoD Regulation 5400.7-R, DoD Freedom of Information Program;
- Bearing current and prior designations indicating controlled access and dissemination (*e.g.*, For Official Use Only, Sensitive But Unclassified, Limited Distribution, Proprietary, Originator Controlled, Law Enforcement Sensitive);
- Technical data, computer software, and any other technical information covered by DoD Directive 5230.24, Distribution Statements on Technical Documents, and DoD Directive 5230.25, Withholding of Unclassified Technical Data from Public Disclosure; or
- Personally identifiable information, such as information protected pursuant to the Privacy Act and the Health Insurance Portability and Accountability Act.

The proposed rule would revise DFARS 252.204-7000, Disclosure of Information, to add definitions for "DoD information" and "nonpublic information." "DoD information" would mean any nonpublic information that "[h]as not been cleared for public release in accordance with DoD Directive 5230.09, Clearance of DoD Information for Public Release," and is either "[p]rovided by or on behalf of [DoD] to the Contractor or its subcontractor(s)," or "[c]ollected, developed, received, transmitted, used, or stored by the Contractor or its subcontractor(s) in support of an official DoD activity." "Nonpublic information" would mean any Government or third-party information that "[i]s exempt from disclosure under the Freedom of Information Act (5 U.S.C. § 552) or otherwise protected from disclosure by statute, Executive order, or regulation," or "[h]as not been disseminated to the general public, and the Government has not yet determined whether the information can or will be made available to the public."

NEW DFARS CLAUSES IN THE PROPOSED RULE

The proposed rule also would add two new DFARS clauses, DFARS 252.204-70XX, Basic Safeguarding of Unclassified DoD Information, and DFARS 252.204-70YY, Enhanced Safeguarding of Unclassified DoD Information, which would be included in contracts (and subcontracts) when a contractor will potentially have unclassified DoD information on its information systems.[1]

The first clause, DFARS 252.204-70XX, Basic Safeguarding of Unclassified DoD Information, would require contractors to implement first-level information technology security measures to protect unclassified Government information from unauthorized disclosure, loss, or exfiltration. These measures include protecting unclassified Government information on public computers or websites, using the best level of security and privacy available for transmitting electronic information (*e.g.*, emails, text messages, blogs), using caution when transmitting voice and fax information, protecting information with at least one physical or electronic barrier (*e.g.*, locked container or room, login and password), clearing information on media that has been used to process unclassified Government information, protecting against intrusions by providing current and updated malware protection services (*e.g.*, anti-virus, anti-spyware) and prompt application of security software upgrades, and transferring information to a subcontractor only when the subcontractor has a need to know the information and has the requisite level of security.

[1] The second clause (DFARS 252.204-70YY) would be included in contracts and subcontracts when a contractor will potentially have unclassified DoD information that is in one of the categories identified above that requires an enhanced level of protection.

The second clause, DFARS 252.204-70YY, Enhanced Safeguarding of Unclassified DoD Information, would require contractors to use enhanced information technology security measures applicable to the encryption of data for storage and transmission, network protection and intrusion detection, and cyber intrusion reporting. These enhanced measures would apply to DoD information in the special handling categories noted above, and would require the contractor to, among other requirements, implement information security controls for its unclassified information systems that meet a specified minimum level of enhanced safeguarding for unclassified DoD information, and use DoD-approved identity authentication credentials.

Contractors would also be required to report to DoD within 72 hours of discovery of any cyber incident that affects DoD information on, or transiting through, the contractor's unclassified information systems. "Reportable cyber incidents" include, among others, incidents involving possible data exfiltration or manipulation or other loss or compromise of DoD information on, or transiting through, the contractor's (or a subcontractor's) unclassified information systems, or other incidents that allow unauthorized access to an unclassified information system with DoD information. Contractors would be required to take specified actions in response to a reported cyber incident, such as reviewing their unclassified networks for evidence of intrusion, reviewing the data accessed during the cyber incident to identify DoD information, preserving images of affected information systems, and cooperating with the DoD Damage Assessment Management Office ("DAMO") to identify systems compromised by the cyber incident.

The proposed rule notably does not address DoD sharing of cyber security threat information with industry. The proposed rule states that this issue may be addressed through follow-on rulemaking, and also notes that on-going federal Government efforts to review and define the scope of controlled unclassified information, which are being led by the National Archives and Records Administration, may require future DFARS revisions.

SIGNIFICANCE FOR GOVERNMENT CONTRACTORS

The proposed rule is significant because, if implemented, it would extend information security requirements for unclassified DoD information to all Government contractors, regardless of their security clearance or ownership status. Because the rule covers a broad range of DoD information, the costs to contractors of reporting security breaches and protecting the information could be significant.[2] As DoD acknowledges in the proposed rule, "most large contractors handling sensitive information already have sophisticated information assurance programs and can take credit for existing controls with minimal additional cost," but "most non-large businesses have less sophisticated programs and will realize costs meeting the additional requirements." DoD estimates that the proposed rule will affect approximately 76 percent of DoD's small business contractors by requiring these contractors to provide protection of DoD information at the enhanced level. Thus, as DoD itself seems to acknowledge, the proposed rule has the potential to impose a fairly significant cost burden on the small business contractor community.

DoD has invited interested parties to submit comments on the proposed rule on or before August 29, 2011. Contractors with insight relating to any aspect of the proposed rule should consider submitting a comment. By submitting comments, contractors can raise their concerns with the proposed rule before it becomes final.

---

[2] *See* "Proposed Rule Would Seek to Help Protect Unclassified DoD Information," 96 Fed. Cont. Rep. (BNA) 5 (2011).

Attorneys at Covington & Burling LLP are experts in advising companies on matters relating to government contracts and information security. We are closely monitoring the proposed rule, and we would be pleased to discuss the proposed rule and its potential impact on your industry, company, and customers. If you have any questions concerning the material discussed in this client alert, please contact the attorneys listed below:

Alan Pemberton	202.662.5642	apemberton@cov.com
David Fagan	202.662.5291	dfagan@cov.com
Scott Freling	202.662.5244	sfreling@cov.com
Heather Finstuen	202.662.5823	hfinstuen@cov.com