wiley

ALERT

Proposed FAR Rule Would Require Contractors to Follow Basic Security Protocols for Information Systems

August 24, 2012

The Federal Acquisition Regulatory Councils (FAR Councils) on Friday issued a new proposed Federal Acquisition Regulation (FAR) rule that would impose basic safeguarding requirements for contractor information systems where information provided by, or generated for, the Government (other than public information) will reside on, or transit through, the contractor's system. *See* 77 Fed. Reg. 51496 (Aug. 24, 2012). The rule would establish a new FAR clause, 52.204-XX "Basic Safeguarding of Contractor Information Systems," which would be included in virtually all contracts in which the contractor is expected to receive or generate non-public government information on the contractor's information systems, including commercial item and commercial item off-the-shelf (COTS) contracts, and would apply equally "to all Federal contractors and appropriate subcontractors regardless of size or business ownership."

The Proposed Rule adopts many of the "basic" requirements that were proposed in the Department of Defense's (DoD) Advance Notice of Proposed Rulemaking on March 3, 2012 and reflects comments that DoD received in response to its proposed rule. *See* 75 Fed. Reg. 9563 (Mar. 3, 2010) (Safeguarding Unclassified Information). The measures adopted for the proposed FAR rule, however, do not include any of the enhanced protection measures or threat disclosure requirements that had been suggested for DoD contractors. The "basic protection measures" contemplated in the Proposed Rule are "first-level information technology security measures used to deter unauthorized disclosure, loss, or compromise" of non-public government information. The Proposed Rule's broad applicability to

Authors

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Practice Areas

Ethics Advice & Compliance Audits and Plans

Government Contracts

commercial item and small business contracts reflects the Government's view that "the first-level protective measures (i.e., updated virus protection, the latest security software patches, etc.) are typically employed as part of the routine course of doing business," so they are not expected to materially add to the burden of doing business with the Government.

The Proposed Rule outlines specific safeguarding requirements and procedures that contractors would be required to follow to secure their information systems and the integrity of government data that resides on or transmits across those systems, including:

- **Public Computers:** Contractors may not use "public computers" (i.e., hotel business centers, airport kiosks, etc.) or computers that do not have access controls to access Government information.
- **Public Web Sites:** Contractors may not post Government information to publicly available websites, or those with access limited only by domain/Internet Protocol restrictions. Contractors would be permitted to post information to web pages that control access via user ID/password, user certificates or other "technical means."
- **Transmitting Electronic Information:** Email, text messaging and other electronic communications must be sent using "technology and processes that provide the best level of security and privacy available, given the facilities, conditions and environment."
- **Transmitting Voice and Fax Information:** Voice and fax transmissions may be made only "when the sender has a reasonable assurance that access is limited to authorized recipients."
- **Physical and Electronic Barriers:** Information systems must utilize "at least one physical and one electronic barrier (e.g., locked container or room, login and password) when not under direct individual control."
- **Sanitized Media:** Electronic media containing Government information must be sanitized or wiped prior to external release or disposal.
- **Intrusion Protection:** Basic "intrusion protection" must be utilized, including current and regularly updated malware protection services, and prompt application of security-relevant software upgrades.

For contractors who find the new FAR clause in their contracts, in addition to comparing the new requirements against the contractor's current security protocols, it may also be necessary to conduct new employee training on data security requirements. The prohibition on accessing Government information from public computers and the email requirements, in particular, may require some employees to alter their IT habits, particularly if they regularly use personal email accounts (such as Hotmail or Gmail) for work or rely on business centers to access data when traveling.

Comments on the Proposed Rule may be submitted through October 23, 2012. Although the proposed FAR clause appears straightforward and applies basic data protection protocols that most contractors likely already employ, there may still be room for improved clarity. In particular, the Proposed Rule includes little guidance about the requirement that contractors transmit electronic information using only "technology and processes that provide the best level of security and privacy available," and it is not clear what standard the

rule would impose or what "best level" means in practice.

The Proposed Rule continues the Government's recent focus on contractors and their role in cybersecurity and data protection. In addition to the proposed DoD rule mentioned above, the Proposed Rule also noted that related proposed rules are still pending, including FAR Case 2011-011, Organizational Conflict of Interest and Contractor Access to Nonpublic Information, and FAR Case 2011-010, Sharing Cyber Threat Information. The DoD also issued a recent interim final rule to enhance its defense industrial base cybersecurity voluntary disclosure program, which was covered in a May 14, 2012 client alert.