wiley

ALERT

New Final Rule Amends the FAR to Require Basic Safeguarding of Contractor Information Systems

May 16, 2016

Today, the GSA, DOD, and NASA published a Final Rule entitled Basic Safeguarding of Contractor Information Systems. The Rule establishes basic safeguarding measures that are generally employed as part of "routine" business practices, and does not affect other specific information safeguarding requirements relating to Controlled Unclassified Information (CUI) or classified information. The Rule "is just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems." In particular, the FAR councils intend to issue a new rule to implement the OMB proposed guidance that emerged last summer. Several of the information systems safeguarding guidelines (discussed below) are drawn from NIST 800-171, which is the same set of standards that OMB recommended in its proposed guidance and that DOD now follows. It is likely that future rulemaking will move industry further towards implementing the NIST safeguards for contractor information systems.

The purpose of the Rule is to impose safeguarding requirements on covered contractor information systems that contain or process information provided by or generated for the Government. Critically, and as distinct from the proposed rule, the focus of the rule is on the safeguarding of the information system itself, and not the information generally. The scope of the Rule was intended to be "very broad, because [the] rule requires only the most basic level of safeguarding."

Practice Areas

Government Contracts

Some commenters criticized the Rule's requirements for being "too basic and rudimentary to achieve the rule's intended purpose," while others expressed concerns that the rule is too vague, and that the lack of clarity incentivizes contractors to design the most stringent security standards so as to avoid disputes with the government. Small business concerns, in particular, expressed concern about the financial impact of complying with intentionally broad safeguarding requirements that are not necessarily typically employed as a matter of routine business practices. The requirements will not, however, apply to Commercial Off the Shelf (COTS) items.

Among other requirements, contractors will be required to ensure that the following information security safeguards are in place for the covered contractor information systems:

- Limit information system access to authorized users, processes, and devices
- Limit information system access to permitted transactions and functions
- Authenticate identities of users, processes, or devices as a prerequisite to accessing organizational information systems
- Limiting physical access to information systems, equipment, and operating environments
- Monitor, control, and protect organizational communications at external boundaries and key internal boundaries of the information system
- Provide protection from malicious code, and update malicious code protection mechanisms "when new releases are available"
- Perform periodic scans of the information system and real-time scans of files from external sources as files are accessed.