wiley

NEWSLETTER

Five Compliance Challenges Clients Face When Implementing NIST 800-171

February 2018

Government Contracts Issue Update

Over the last several months, the acquisition community has been working to implement DFARS 252.204-7012, and in particular, the requirement to provide "adequate security" as set forth in the 110 security controls in NIST 800-171. In the course of advising clients on the December 31, 2017, deadline to implement these security requirements, many common themes and challenges emerged. This article highlights five of those issues involving the scope and documentation of compliance, and resolving ambiguities among the security controls.

Can I Segregate My Covered DOD Information System from my Commercial Systems?

This is possible and, for some contractors, may be a viable way to harden a system used for DOD contracting while avoiding a complete redesign of other existing commercial systems. The challenge is determining where one system ends and others begin. NIST provides some guidance on determining information system boundaries in NIST SP 800-37r1 Section 2.3, which provides factors to consider such as whether systems have the same management control, mission objectives, and operating environment. This guidance, however, is high level and does little to address the complexities of network architecture in the real world. Contractors looking to segregate a DOD system would be prudent to document clearly how they determine the boundaries between information systems.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Government Contracts
Privacy, Cyber & Data Governance

What Information Systems Are Covered?

Often the hardest challenge contractors face is determining whether an information system is processing covered defense information (CDI) and is therefore within the scope of DFARS 252.204-7012 and must meet NIST 800-171. For contractors with multiple information systems, determining which systems process CDI may not be obvious. The definition of CDI includes Controlled Technical Information as well as Controlled Unclassified Information, as defined by the registry maintained by the National Archives and Records Administration. For information that is marked in the contract, this is an easy determination. But, the DFARS clause also includes CUI that is "collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." This could sweep in wide swaths of information that is created or received by the contractor, but not marked. Contractors may benefit from focusing on other aspects of the CDI definition to narrow the scope of information that may be within its scope, such as whether the information is "in support of the performance of the contract," which may help clarify if the information at issue brings an information system into the scope of the DFARs clause.

How Do I Determine If I Have Complied With NIST 800-171?

NIST 800-171 has both the virtue and vice of being flexible. The security controls were purposefully designed to be technology-neutral and to allow for a range of solutions, giving contractors the ability to right-size and tailor the controls. While that has the clear benefit of allowing contractors to implement NIST 800-171 in the manner that works best for their company, the downside is that compliance is not always readily apparent. DOD does not certify compliance, and it has not authorized a third-party certification process. Given this lack of formal certification, industry has turned to a variety of methods to document compliance, including structured internal audits and consulting with outside vendors who can provide a level of external verification.

What Do I Do If I Have Identified Gaps?

DOD has recognized that not all contractors will meet all NIST 800-171 security controls. The preferred method for identifying gaps is to create a System Security Plan (which is required by control 3.12.4) and document any gaps in Plans of Action and Milestones (POAMs). These POAMs will vary in detail based on the nature and scope of controls to be implemented and should reflect the realities and challenges of implementing these controls. At a minimum, they should provide some indication that the company has a workable path to address the gaps and implement required controls. While POAMs provide short-term relief for some gaps, DOD's guidance suggests that it considers these controls to be a "minimum," and is expecting contractors to be realistically working towards implementation.

How Do I Address Ambiguities in the Security Controls?

Many of the security controls in NIST 800-171 are ambiguous. Given the risk of breaching contractual duties and potential False Claims Act liability for failing to implement these controls when required, this ambiguity makes it all the more important to document the good faith steps contractors are taking to comply. While there may be no silver bullet solution, the controls in NIST 800-171 are mapped to NIST 800-53, which provides additional structure to the controls. First, each control in NIST 800-53 has "Supplemental Guidance" that

provides a level of further description. Also, most of the controls in NIST 800-171 map to a only couple of the "Control Enhancements" in each control in NIST 800-53. It may be reasonable for contractors to conclude that any Control Enhancements that are not expressly mapped are not required, which would limit the burden and ambiguity in implementing NIST 800-171.