DFARS contract clause 252.244-7001 (“Contractor Purchasing Systems”) establishes 24 adequacy criteria. A “significant deficiency” in any one of those criteria will lead to a disapproved purchasing system and possible payment withholds. As readers may know, in 2014 the clause was revised to add adequacy criteria related to compliance with the requirements of DFARS contract clause 252.246-7007 (“Contractor Counterfeit Electronic Part Detection and Avoidance System”) (CEPDAS). We wrote about the new criteria (with a certain air of smugness, since we had predicted the increased emphasis on the area) in **this article** .

The point is, a CPSR doesn’t just cover purchasing files. It covers a wide range of requirements including compliance with CEPDAS and compliance with Item Unique Identification (IUID). If you think your Supply Chain Management department can pass a CPSR on its own, think again.

And now comes word that CPSRs are getting even harder. On January 21, 2019, Under Secretary of Defense (Acquisition and Sustainment) Ellen Lord issued a **Memo** that directed DCMA to “validate, for contracts for which they provide contract administration and oversight, contractor compliance with the requirements of DFARS clause 252.204-7012.” That DFARS contract clause, for those who don’t know, is the Cybersecurity clause, known more formally as “Safeguarding Covered Defense Information and Cyber Incident Reporting.”

Consequently, when CPSRs are performed, reviewers will be assessing how well contractors are complying with cybersecurity requirements.

According to the Memo, reviewers will—

-

Review contractor procedures to ensure contractual DoD requirements for marking and distribution statements on DoD CUI flow down appropriately to their Tier 1 Level Suppliers.

-

Review Contractor procedures to assess compliance of their Tier 1 Level Suppliers with DFARS Clause 252.204-7012 and NIST SP 800-171.

According to a client alert from attorneys at Crowell & Moring, “the scope of DCMA’s review appears broader than the Clause’s textual requirements.” To us, this means that CPSR adequacy may hinge on more than complying with the requirements of the clause itself, which is not good news for contractors.

Importantly, the actual Purchasing System clause was not rewritten. There are no additional adequacy criteria. The cybersecurity review steps appear to be “unwritten” adequacy criteria. Consequently, we don’t know what happens if a contractor doesn’t pass the cybersecurity review steps. Will a system be failed? Will payment withholds be implemented? We just don’t know.

But if history is any guide, it is just a matter of time until the clause is revised (again) to add cybersecurity to IUID and CEPDAS requirements. Meaning, of course, that it will become even harder to pass a CPSR, and that it will require even more cross-functional support to do so.