The information security standard set forth by the National Institute of Standards and Technology (NIST), known as NIST SP 800-171, has experienced multiple revisions since its original publication in June 2015. Following these changes, many individuals are left wondering where their company stands with compliance and what steps they must take next. The following brief history and explanation of NIST 800-171 is meant to clarify these and other questions about the standard.

In August of 2015, the Department of Defense (DoD) added an interim rule to the Defense Federal Acquisition Regulation Supplement (DFARS) which required all relevant companies with government contracts to comply with NIST 800-171 under clause 252.204-7008 and 252.204-7012. The original NIST 800-171 publication contained 109 controls that contractors had to comply with for all systems that contained Covered Defense Information (CDI), which includes Unclassified Controlled Technical Information (UCTI) and other categories of non-classified information that require special handling.

Since its release, NIST 800-171 has been superseded by NIST 800-171 Revision 1, published in December 2016 and further updated in November 2017. Among terminology changes, Revision 1 also included the addition of a new control (now 110 in total), as well as specific requirements for how a company can reach compliance. These requirements include the completion of an assessment of cybersecurity compliance, a System Security Plan (SSP), a Plan of Action and Milestones (PoAM) and an Incident Response Plan (IRP).

On September 21, 2017, the Office of the Under Secretary of Defense released a memorandum which stated that, under the DFARS clause, contractors must implement the version of the standard that was in effect at the time of contract award. Meaning, if a company signed a contract after Rev. 1 was in effect, they will follow the updated guidelines. If a company signed a contract before Rev. 1 was in effect, they may choose to leave their contract as it is or work to have their contract revised. Contractors then must work with contracting officers to modify their contracts to authorize use of the most recent version of 800-171.

To help with these contract modifications, the Office of the Under Secretary of Defense released a second memorandum on December 15, 2017 which requested that contracting officers handle contract revisions via the mass modification system. This system automates contract revisions electronically, making modifications simpler to identify and accomplish.

To put it briefly, as it stands now, all companies who have contracts containing DFARS clauses 252.204- 7008 or 252.204-7012 and handle CUI should know the following information about the standard:

- Contractors are bound to the version of NIST 800-171 that was published at the time of contract signage. However, without contract modification, they are potentially not protected or compliant based on current revisions.
- Contracts signed under the original NIST 800-171 standard cannot necessarily consider completion of an SSP and PoAM as proof of compliance, as these documents were not listed as requirements in their contract. Contracts must first be modified in order to use these documents as proof of compliance.
- Contractors can solicit their contract officers to have their contracts modified to include the latest version of 800-171, which will most likely be handled through the mass modification system.

The Wisconsin Manufacturing Extension Partnership (WMEP) is available to assist companies who need to create and implement an SSP and PoAM.