Defense Contractors Are Required To Implement Cybersecurity Measures In Order To Do Business with the Federal Government

Articles, Privacy, Technology and Data Security September 14, 2020

By Mark Hamilton

The Defense Federal Acquisition Regulation Supplement ("DFARS") 252.204-7008 and 252.204-7012 require defense contractors who possess, store or transmit "covered defense information" to comply with the security requirements set forth in the U.S. National Institute of Standards and Technology ("NIST") Special Publication 800-171 ("SP 800-171). "Covered defense information" includes unclassified controlled technical information of the type contained in drawings related to the manufacture of defense articles.

These DFARS clauses contain a flow down provision that requires defense contractors to incorporate these clauses into their contracts with any subcontractors who provide "operationally critical support" or whose subcontracts otherwise involve covered defense information.

These regulations also require companies to report the discovery of any "cyber incidents" that affect either a contractor's computer system or the covered defense information stored in the contractor's computer system. This means that the US Government expects even second and third-tier contractors to report any incidents in which their computer systems are compromised.

To recap, if your company is working on defense contracts, it is required to implement SP 800-171 in order to comply with the relevant DFARS cybersecurity requirements. This is true even where your company is merely a second or third-tier contractor because the prime contractor is required to flow down these DFARS clauses to its subcontractors.

The implementation deadline for SP 800-171 was December 31, 2017. So if your company is not yet compliant, do not wait for the next time sensitive purchase order to arrive before taking action. For additional information contact Mark Hamilton.