What You Need to Know About the DFARS Cyber Security Requirements

In 2015, The Office of Personnel Management released that it was hacked and that 21,500,000 personally identifiable records of government employees, contractors, and their families were stolen. In response, the Department of Defense (DoD) adopted a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to protect covered defense information. The final rule requires covered DoD contractors who utilize cloud computing services to adhere to cloud computing requirements of 252.239-7010, implement security requirements of the NIST SP 800-171, and report any cyber breach within 72 hours of its discovery to the DoD as soon as practical, but no later than 12/31/2017.

The final rule states that whenever a covered contractor uses cloud computing to provide IT services during a DoD contract the covered contractor must comply with DFARS 252.239-7010. Whenever a contractor or subcontractor stores or transmits covered defense information on a cloud-based IT environment, the cloud service provider they use must meet or exceed the Federal Risk and Authorization Management Program (FedRAMP) standard for moderate compliance and also the DFARS 252.204-7012 cyber incident reporting requirements that the contractors and their sub contractors must comply with. This means that many contractors and subcontractors who currently uses cloud service providers will have to substantially modify their service level agreements (SLAs) and terms and conditions with them to gain assurance that the cloud service provider meets the final rule's standards.

The crux of DFARS 252.204-7012 is that contractors and their sub contractors provide adequate security commensurate with the consequences and probability of loss, misuse, or unauthorized access of, or unauthorized modification of information. To accomplish adequate security, the final rule requires that contractors and their sub contractors implement the controls outlined in the NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations as soon as practical, but no later than 12/31/2017. The final rule also requires that contractors report cyber incidents to the DoD within 72 hours of its discovery. Further, it also requires the contractor to attempt to isolate and capture any malicious software found on the contractor's IT system and provide the DoD access to the contractor's system at the DoD's discretion.

An amendment to DFARS 252.204-7012 in 2016 provides procedures for contractors to request limited exemptions from specific NIST SP 800-171 requirements. A covered contractor can note that a specific control is nonapplicable or that the contractor has an alternative, but equally effective measure in place to provide adequate security. Contractors must submit written requests to their Contracting Officers prior to the contract being awarded to vary from NIST SP 800-171. A representative of the DoD CIO will review and adjudicate those submitted variations.

By: Stahler Heath, ARSA IT Services