UPDATE - DoD Allows Additional Time for Compliance With Multifactor Authentication Requirement of Defense Cybersecurity Rules

By: Benjamin J. Lambiotte

Last month, we reported on DoD's adoption of an interim rule and standard contract clauses on Safeguarding Covered Defense Information and Cyber Incident Reporting. *See http://www.gsblaw.com/pdfs/DoDAdoptsNewCyberSecurityRulesFinal.pdf*. One of the major provisions of the rule is that the IT systems of covered contractors and subcontractors must comply with the security requirements of NIST SP 800-171 – "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (*See* http://dx.doi.org/10.6028/NIST.SP.800-171). These requirements include 3.5.3 "Use of multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts."

On October 8, 2015, DoD issued a class deviation, which allow covered contractors and subcontractors up to **9 months** after contract award to comply with the multi-factor access authentication requirement.

According to SP 800-171 3.5.3: "Multifactor authentication" requires two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic device, token); or (iii) something you are (e.g., biometric)." Multifactor authentication may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials. There are a number of solutions available commercially.

Offerors must notify the contracting officer in the bid if they anticipate needing the additional time allowed.

Read the deviation here: http://www.acq.osd.mil/dpap/policy/policyvault/USA005505-15-DPAP.pdf