DFARS 2021 Cybersecurity - Awards in 2021 Require an Assessment Score on File with the Supplier Performance Risk System

On September 29, 2020 the DOD updated the Defense Federal Acquisition Regulation Supplement (DFARS) Cybersecurity rules covering DOD contractors and subcontractors. Under the new DFARS cybersecurity rule, after Nov. 30, 2020 all contractors and subcontractors handling drawings, specifications or other CUI must file a current DOD Assessment Management (DoDAM) score prior to receiving an award.

DoDAM scores quantitatively assess compliance with the 110 requirements of NIST 800-171, rev. 2. Scores must be filed in the Supplier Performance Risk System (SPRS) and be available to all DOD Contract Officers before any award. Scores below 110 (full compliance) must include a date for full compliance. False or inaccurate claims of compliance may be subject to the federal False Claims Act (FCA). In 2019, FCA penalties exceeded $3 billion.

Is your mandatory DOD Assessment Methodology Score Over 100?

Does your NIST 800-171 cybersecurity documentation validate your score?

Many contractors have been claiming NIST 800-171 compliance since the first requirements in late 2017. Contractors audited in 2019/2020 by the Defense Contractors Management Agency (DCMA) were asked to produce the mandatory System Security Plan (SSP) documentation to support their claims. “And according to Katie Arrington, CISO DoD Acquisition Office, about 80% of those contractors audited have failed the audit.”

It is understandable that 80% of small contractors would fail to adequately document the 110 NIST cybersecurity policy and procedure documents. The DOD estimates the cybersecurity documentation effort required for small contractors to create an SSP and related POAM covering the 110 NIST 800-171 requirements at 110 hours. DOD SBIR contractors who have attempted this documentation put the actual level of effort much higher, in the range of 300-400 hours per small contractor site.

A partial set of the necessary NIST support documents is shown at right. Although very well written, their highly technical typically 18th grade verbiage can be more intimidating than useful to small fabricators and assemblers.

The highly automated ACR 2 Cybersecurity Risk Management System™ (ACRMS™) software and services package has been used since 2006 to assist small organizations to meet federal cybersecurity requirements for protecting sensitive information. Using the ACRMS™ software ACR 2 has been able to help dozens of small (typically <10 staff) DOD contractors to cost effectively meet their required DFARS cybersecurity

System Security Plan and POAM documentation in less than 30 hours.

ACRMS™ costs are modest with 30 hour video augmented policy creation packages starting at **$2495 for up to 50 staff.** Follow-up task management software supporting the typically hundreds of hours of effort needed to maintain a fully compliant NIST 800-171 compliance program starts at **$150/month**. For more information email info@acr2solutions.com or see our CUI website at

https://CUIcybersecurityCompliance.com.