ACR 2 Cybersecurity Risk Management System™ (ACRMS™) for DFARS 252.204-7019 Compliance Rapid, Cost-effective CUI Cybersecurity

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 requirements of 252.204-7019, after Nov. 30, 2020 all contractors and subcontractors handling CUI must file a current DoD Assessment Management (DoDAM) score prior to receiving a contract award or update or extension.

DoDAM scores quantitatively assess compliance with the 110 requirements of NIST 800-171, revision 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. Fraudulent claims of compliance may be subject to the federal False Claims Act (FCA). In 2019, FCA penalties exceeded $3 billion.

The new DFARS cybersecurity rules are based on National Institute of Standards and Technology (NIST) Special Publication 800-171 revision 2 and its' reference documents. A partial set of these cybersecurity documents is shown at left.

There are five parts to DFARS cybersecurity compliance;

1. Create policy/procedure documentation covering the 110 NIST requirements.
2. Implementation of policy safeguards such as encryption and security training.
3. Create a System Security Plan (SSP) tracking status of the cybersecurity controls, along with a Plan of Actions and Milestones (POAM) detailing a strategy for achieving all missing or incomplete cybersecurity controls and safeguards.
4. Calculate the DoD Assessment score.
5. Assign and schedule about 130 cybersecurity maintenance tasks.

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.

In working with a set of 44 small AFRL contractors it was found that most had NIST 800-171 technical safeguards in place. None of the contractors had an SSP, POAM or more than minimal cybersecurity documentation. Using the ACRMS™ contractors were able to create

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

The 110 NIST 800-171 cybersecurity requirements generate about 130 daily, weekly, monthly or annual tasks. Mandatory tasks range from daily virus updates to weekly network audits to annual incident simulations and policy updates. These recurring "allowable costs" tasks involve hundreds of annual labor hours even for two or three person DoD contractors. The ACRMS™ helps track the tens of thousands of dollars of annual reimbursable costs.

ACRMS™ costs are modest and ACRMS™ video augmented policy creation packages start at $1795 for up to 50 staff. For more information or to purchase see our CUI website at

https://CUIcybersecurityCompliance.com