



ACR 2 Solutions Cybersecurity Risk Management System™ (ACRMS™) for DFARS 2021 Cybersecurity Compliance

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, after Nov. 30, 2020 all contractors and subcontractors handling 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. Fraudulent claims of compliance may be subject to the federal False Claims Act (FCA). In 2019, FCA penalties exceeded \$3 billion.



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

There are five parts to DFARS 2020 cybersecurity compliance;

1. Create policy/procedure documentation covering the 110 requirements.
2. Implementation of policy safeguards such as encryption and security training.
3. Create a System Security Plan (SSP) tracking status of about 135 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 the 95-120 weekly, monthly, quarterly or annual tasks necessary to maintain a high DOD Assessment score during a contract.

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.

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

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

ACRMS™ costs are modest and video augmented policy creation packages start at \$3495 for up to 50 staff. Cybersecurity costs generally qualify as allowable costs under DoD and other federal contracts. For more information and cost data see our CUI website at

<https://CUIcybersecurityCompliance.com>