DFARS and FAR Cybersecurity 2022

ACRMS™ for DFARS 252.204-7012 and FAR 52.204-21 Cybersecurity Compliance for NIST Manufacturing Extension Partnership (MEP) Clients

Federal Cybersecurity Requirements for FY 2022: In 2022 Department of Defense (DoD) contracts involve 3 types of non-public information. Federal Contract Information (FCI) is non public information that requires only minimal cybersecurity. Seventeen cybersecurity requirements taken from NIST 800-171 are described in FAR 52.204-21. Policies to carry out these requirements will typically involve 35 or so daily, weekly, quarterly or annual tasks to implement and maintain the 17 safety controls. About half of the 80% of small DoD contractors under 20 staff handle only FCI.

Controlled Unclassified Information or CUI includes drawings, specifications, catalog lists and similar information. Loss of enough CUI can amount to the equivalent of a classified data breach. DFARS 252.204-7012 requires contractors handling CUI to implement and maintain all 110 safety controls of NIST 800-171. About 80,000 small DoD contractors are believed to handle CUI.

Classified data is handled by very few DoD contractors and is outside the scope of this discussion.

FCI Cybersecurity Compliance: FCI cybersecurity compliance can be achieved in a one day Boot Camp. Policies to achieve the 17 requirements can be written in less than a day of online group instruction, including setup of a task management system to implement and maintain these policies. Under FAR 21 cybersecurity tasks are explicitly allowable costs.

Initial DFARS Cybersecurity Compliance: DFARS 252.204-7012 requires “adequate security”, starting with a System Security Plan (SSP) and a Plan Of Actions And Milestones (POAM) addressing the 110 safety controls listed in NIST 800-171, now in rev. 2. SSPs are given scores of 1, 3 or 5 for each of the 110 requirements that is fully implemented and maintained. SSP assessment scores must be filed in the Supplier Performance Risk System (SPRS) database.

Full DFARS Cybersecurity Compliance: Typically for a small contractor there will be about 240 daily, weekly, monthly quarterly and annual tasks required to implement and maintain the 110 mandatory safety controls. Initial SSP scores are often in the 10 to 30 range. Achieving full 110 point compliance generally requires an additional 6-12 months.

Initial DFARS Compliance Problem: As of May 5, 2022 only 19.905 of an estimated 80,000 contractors had completed and scored their SSPs. DoD estimates (optimistically) 110 to 304 hours for preparation of an SSP/POAM package for small contractors. A partial set of the applicable NIST protocols is shown at right.

Initial DFARS Compliance Solution: The ACR 2 Cybersecurity Risk Management System™ (ACRMS™) 3-day Boot Camp can bring small (<50 staff) DoD contractors into

initial DFARS compliance in 21 hours for $500/site.

ACRMS™ 3-day, 21-Hour Boot Camp: Originally developed and demonstrated for the AFRL SBIR program, the 3-day ACRMS™ Boot Camp was able to bring 44 small contractors, average size 9.6 staff per site, into initial compliance with DFARS 252.204-7012. This cybersecurity requirement was later expanded to include all of the approximately 80,000 DoD small contractors handling CUI.

Full Compliance Support From NIST Manufacturing Extension Partnership (MEP) Cybersecurity Programs: Initial SSP/POAM preparation is similar for most small contractors. Moving from initial compliance scores of 30 or 40 to full 110 point compliance often requires specialized and highly technical efforts. The NIST MEP Cybersecurity programs are major technical support resources for US contractors. Following an initial SSP/POAM, the MEP centers can provide subsidized and customized support services to help contractors move into full DFARS compliance.