ACRMS™: $100/month DFARS Cybersecurity Mgt. for 1-2 Person Federal Contractors

The ACR 2 Solutions Cybersecurity Risk Management System or ACRMS™ is a cybersecurity management solution tailored for small Federal contractors to meet DFARS (Defense Federal Acquisition Regulation Supplement) requirements at an affordable cost. In a 44-site Air Force SBIR contractors project, half of the contractors had all, or most, of the required technical safeguards. None of the SBIR awardees had more than 1/3 of the administrative controls. Under the NIST cybersecurity point scoring system, technical controls count for less than a quarter of the total points.

DFARS Cybersecurity Compliance: DFARS 252.204-7012 is part of most DoD contracts involving Controlled Unclassified Information or CUI. DoD estimates that 59,659 small contractors handle CUI. In January 2025, GSA proposed extending the 110 NIST 800-171 cybersecurity requirements to all federal contractors.

There are approximately 400,000 Federal contractors, with almost 43% or 175,000 having only 1 or 2 staff. Another 39% have 3 to 25 staff, with the last 20% having 26 or more employees. Also, some large contractors have setup CUI enclaves with 1-2 staff.

DFARS 252.204-7012 requires 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. A partial set of the applicable NIST guidance documents is shown at right.

ACRMS™ Program: The ACRMS™ order form and required mutual Non-Disclosure Agreement are available on the ACRMS™ project page at https://cuicybersecurity compliance.com/documents.

As shown at right on the Order Form, the ACRMS™-VSS program begins with a $75 (1 to 2 staff) rapid online guided risk assessment and System Security Plan (SSP), ending with a SPRS score.

ACRMS Initial Risk Assessment for Very Small (1-2 Staff) sites. Includes 1.5 hour initial risk assessment, System Security Plan, and SPRS Score calculation meeting. Requires signed Non-Disclosure Agreement and registered attendance at ACRMS small site cybersecurity management webinar, either live or recorded. - Credit card only.	$ 75.00
ACRMS Provisioning - DFARS 252.204-7012 Initial Compliance policy package setup with Initial Site Manager Training for Very Small (1-2 Staff) sites - One time price. Credit card or check.	$ 175.00
ACRMS Ongoing Policy, SSP & POAM Updating, Task Management System, updates, and Technical Support for Very Small (1-2 Staff) sites. Includes 20 minute monthly review and assesment update meetng. - month by month license , one month cancellation notice required- credit card required.	$ 100.00

Risk Assessment Results: The initial System Security Plan and risk assessment report describes in detail what is expected of the contractor. It is estimated that up to 30% of newly regulated small contractors may choose to leave the federal market rather than attempt the new cybersecurity requirements. The $75 initial program cost allows contractors to see, in detail, what they will now be required to do if they remain in the federal market. The only cost to the contractor would be the $75 flat fee for the original CUI 3.11.1 risk assessment and CUI 3.12.4 System Security Plan.

Full DFARS Compliance: Contractors wishing to proceed to full NIST 800-171 compliance may purchase a 3-year bundle for $100/month, as shown on the price list.

Larger Contractors: Larger contractors with 3 to 25 can use similar techniques at higher cost. The Order Forms lists initial assessment costs of $225 for contractors between 3 and 25 staff. A 3-year compliance bundle costs $175 per month. Contractors with more than 25 staff are urged to call for pricing.

Small DFARS Enclave: It is typically necessary to separate CUI from other data, as shown in the example at right. Even highly sophisticated university research systems have not been able to adequately secure large and complex networks to DFARS cybersecurity standards.

Win 11 FIPS 140-2 Encrypted Storage - Bitlocker

FIPS 140-2 UTM

Encrypted USB Drive
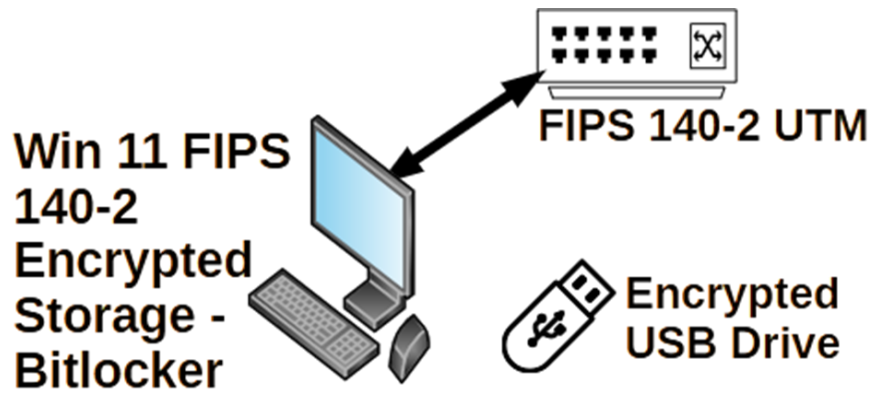
Penn State paid a $1.25 million fine for DFARS cybersecurity failure, while GTRI is defending a potential $19 million FCA lawsuit, not including possible triple damages. In fiscal year 2024, the DOJ recovered $93 million from DOD contractors, not including a $428 million settlement with an aerospace firm after the fiscal year ended.

Liability and Subcontractor Management: In 2025, Cybersecurity requirements must be "flowed down" to all suppliers and subcontractors handling CUI, including any drawings and specifications.

Contractors always remain liable for data security by subcontractors.

The ACRMS™ Enterprise console can provide near real-time monitoring of subcontractor cybersecurity status. It is always better to know than to guess about legal liabilities.

Ongoing Compliance Monitoring and Management: A typical small DoD contractor may have between one and five subcontractors subject to FCI or DFARS cybersecurity requirements. The ACRMS™ Enterprise Edition console allows near real time management of subcontractor cybersecurity using the NIST 800-30 protocol required in CUI 3.11.1. A 10-site example is shown at right. The ACRMS™ console can track both DFARS 252.204 – 7012 and FAR 52.204–21 compliance.

The ACRMS™ Enterprise Edition is based on an expert system AI implementation combining the NIST 800-30 risk assessment protocol and a selection of NIST 800-53 cybersecurity safety controls appropriate for either FCI or CUI. A discussion of the application of this AI technology is available on the videos page of the ACRMS™ project website, https://cuicybersecuritycompliance.com/videos.

Maintaining Full DFARS Cybersecurity Compliance: For a typical small contractor there will be about 230 daily, weekly, monthly, quarterly, and annual tasks required to implement and maintain the 110 mandatory safety controls. Obvious daily tasks include locking the door, setting the alarm and feeding the guard dog. Failing to do daily tasks leads to obvious problems, as shown at right.

SSP Scoring and Monthly Updating: DFARS compliance requires writing policies for the 110 NIST 800-171 requirements. Each policy requirement has a point score between 1 and 5. Total scores can range from +110 to –203. Initial SSP scores are often in the –30 to +30 range. Achieving full 110-point compliance often requires an additional 6-12 months. On the other hand, failure to conduct daily, weekly, and monthly tasks drops scores by 77 points. No task maintenance for 3 months drops scores by 143 points. ACRMS™ risk assessments auto-update every 30 days.

Monthly Online Review Meetings: ACRMS™ support contracts include a 20-minute monthly review. Auto-updated SSP scores are reviewed, and recommendations are made for improvements or updates.