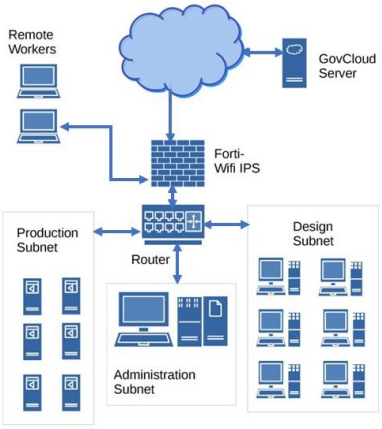
Achieving, Maintaining and Documenting DFARS Cybersecurity Compliance Utilizing MEP and AA Services

Achieving DFARS Cybersecurity Compliance: Complying with DFARS 252.204-7012 is not easy. A fully compliant site will satisfy 110 requirements of NIST 800-171 rev. 2, as documented in a System Security Plan or SSP. Each of the 110 requirements has a point score of 1, 3, or 5 points, since obviously not all precautions are equally important. SSP scores range from 110 at full compliance down to -203. Average DoD contractor scores reported in the 2022 Cyberoam survey, for the 44% of contractors who reported scores, were -23.

Typically, getting to 110 points takes 6-12 months after an initial SSP score of -20 or so. This is entirely expected. Full 110 point compliance requires you to take precautions that were never before requested. Support from a MEP or AA can be very helpful in achieving full compliance.

Boot Camps for Initial DFARS Cybersecurity Compliance: While it is possible, if expensive, to create System Security Plans using a traditional "expert with a briefcase" approach, the typically $15,000 to $30,000 cost is prohibitive for the 300,000 small businesses that form most of the Defense Industrial Base (DIB). More cost effective Boot Camp style approaches include the 9 day $2500 Totem DFARS Workshop and the 16 hour $495-$995 ACR 2 Cybersecurity Management System (ACRMS™) Video Boot Camp.

Typical DoD Small Business Contractor: The ACRMS™ Video Boot Camp uses a typical DoD contractor to provide examples of safeguard implementation. The totally fictional "Bobby Lee Welding" or BLW is a composite of about 50 DoD contractors cybersecured by ACR 2 Solutions since 2017 when DFARS 252.204-7012 went into effect.



A network diagram for BLW is shown at right. The main location has 15 staff, with 2 more in a remote home office location. Over 40% of federal contractors have 1 or 2 staff. Less than 27% have more than 15 staff. The two office locations of BLW are representative of about 70% of small federal contractors.

Both BLW locations are covered by the main site SSP and SPRS scores. The remote home office accesses CUI only by VPN communication with the Forti-Wifi Intrusion Prevention System. The IT Manager and Compliance Officer are both located at the main office in Georgia.

Maintaining DFARS Cybersecurity Compliance: Achieving 110 point compliance is a major achievement, and the temptation is to stop working and celebrate. Not really a good idea.

If your initial score is 110, and you do none of the 4 daily tasks, tomorrow your score will drop from 110 to 88.

If you don't do the 5 weekly tasks, your score drops to 53.

And if you neglect the monthly and quarterly tasks, your score drops to -20, which is where you were a year ago.

Incentives for Cybersecurity for Small Business: Small businesses form a critical portion of the DoD and a very large fraction of the American economy. Both criminal organizations and state actors such as China and North Korea are actively seeking American technology and financial assets.

Microsoft recently published an alert about the Chinese hacking group called Volt Typhoon. "Microsoft's alert revealed that since mid-2021, Volt Typhoon has been targeting the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors in Guam and elsewhere in the U.S.

Increasingly state, local, and federal contracts are requiring cybersecurity for all their contractors, as are many prime contractors. If you lock the doors of your business you probably need to lock up your information assets also.

Using the ACRMS™ to Maintain DFARS Compliance: The updated ACRMS™ sends out compliance reminder emails on a weekly, monthly and quarterly basis. These email reminders will typically go to the Compliance Officer and the IT Manager, who may be the same person in a small company. At Bobby Lee Welding, Bobby Lee is the Compliance Officer while Tommy Lee is the IT Manager.

Log Daily, Report and Update Weekly: Once each week a memo goes out to the BLW IT Manager Tommy Lee and the Compliance Officer Bobby Lee. The IT manager has four daily or weekly tasks as listed below.

NIST 800-53 Safeguard	Assignee	Documents	Task Description
AU-9(4) BACKUP	IT Manager	CUI 3.3.9 AU9(4) moyr.pdf.pdf	The IT Manager sets the system to <daily> backup of encrypted audit data. Note actual backup.
CA-7 CONTINUOUS MONITORING	IT Manager	CUI 3.12.1 3.12.2 3.12.3 3.12.4 CA2 5 7 PL2 moyr.pdf	Report the security status of organization and the information system to <Compliance Officer> on a <daily> basis.
SI-3 MALICIOUS CODE PROTECTION	IT Manager	CUI 3.14.4 3.14.5 SI3 8 moyr.pdf	Malware detection signatures for the Deep Packet Inspection firewall shall be updated <daily>. Note actual updates.
AU-7 AUDIT REDUCTION AND REPORT GENERATION	IT Manager	CUI 3.3.6 AU7 moyr.pdf	The <IT Manager> reviews audit logs on a <weekly> basis and prepares a summary report for review by the <Compliance Officer>.

The weekly reminder email for the IT Manager is saved as a text file and used for reporting purposes. Taking the tasks individually;

1. The IT Manager sets the system to <daily> backup of encrypted audit data. Note actual backup by checking the box on the text copy of the reminder email.
2. Malware detection signatures for the Deep Packet Inspection firewall shall be updated <daily>. Note actual updates by checking the box on the text copy of the reminder email.
3. Report the security status of organization and the information system to <Compliance Officer> on a <daily> basis, either verbally or by phone. Record status updates by checking the box on the text copy of the reminder email.

4. The <IT Manager> reviews audit logs on a <weekly> basis and prepares a summary report for review by the <Compliance Officer>. The <weekly> audit log report is merged with the marked up copy of the reminder email and sent by email to the Compliance Officer.

A draft IT Manager weekly reminder email Form is shown below.

	Monday	Tuesday	Wednesday	Thursday	Friday
Confirm daily backup of encrypted audit data (check or note time).					
Confirm daily update of malware signatures ((check or note time).					
Confirm security status of organization and the information system reported to Compliance Officer (check or note time).					

The five daily or weekly tasks assigned to the Compliance Officer are listed below.

NIST 800-53 Safeguard	Assignee	Documents	Task Description
AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING	Compliance Officer	CUI 3.3.1 3.3.2 AU2, 3, 3(1), 6, 12 moyr.pdf	Audit records shall be analyzed <weekly> by the <Compliance Officer> and summary reports supplied to management and filed in the ACRMS Documents Management System.
CA-2 SECURITY ASSESSMENTS	Compliance Officer	CUI 3.12.1 3.12.2 3.12.3 3.12.4 CA2 5 7 PL2 moyr.pdf	Read status report from <IT Manager>. Create <daily> reports memos for security assessments. File merged memos weekly in Document Management Center
AC-22 PUBLICLY ACCESSIBLE CONTENT	Compliance Officer	CUI 3.1.22 AC22 moyr.pdf	The <Compliance Officer> shall review publicly accessible information on a <weekly> basis to ensure that non-public information is not included. Create memo and file weekly in Document Management Center.
PE-06 MONITORING PHYSICAL ACCESS	Compliance Officer	CUI 3.10.1 3.10.2 PE2 5 6 moyr.pdf	Physical access logs shall be maintained and reviewed <weekly> or when an incident is suspected.
SI-2 FLAW REMEDIATION	Compliance Officer	CUI 3.14.1 3.14.2 3.14.3 SI2 3 5 PM16 moyr.pdf	System flaws or anomalies shall be promptly reported (within 3 days) to the Compliance Officer for investigation by the IT Manager.

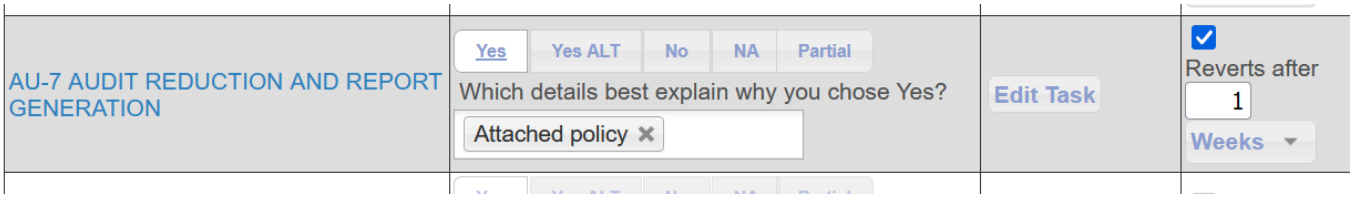
Taking the five tasks individually gives the list shown below.

1. Audit records shall be analyzed <weekly> by the <Compliance Officer> based on information supplied by the <IT Manager>. Summary reports will be supplied to management and signed and dated copies filed in the ACRMS™ Documents Management System.
2. Read security status report from <IT Manager>. Create <daily> reports memos for security assessments. File merged memos <weekly> in Document Management Center.

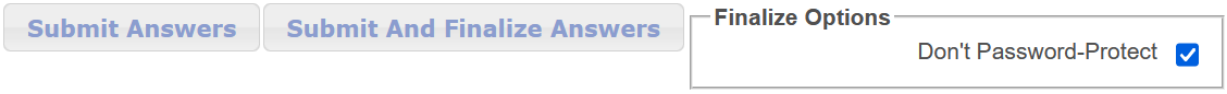
3. The <Compliance Officer> shall review publicly accessible information on a <weekly> basis to ensure that non-public information is not included. Create memo and file <weekly> in Document Management Center.
4. Physical access logs shall be maintained and reviewed <weekly> or when an incident is suspected. Create memo and file weekly in Document Management Center.
5. System flaws or anomalies shall be promptly reported (within <3> days) to the <Compliance Officer> for investigation by the <IT Manager>. Create memo and file upon occurrence in Document Management Center.

Once a week the Compliance Officer will log in to the ACRMS™ site and upload to the Document Management System memos on audit records, security status, publicly accessible information, physical access and system anomaly reports, if an anomaly occurs.

After the uploads the Compliance Officer shall update AU-9(4), CA-7, SI-3, AU-7, AU-6, CA-2, AC-22, PE-6, and SI-2, all of which would otherwise revert to “No”.



After the updates click on “Submit and Finalize Answers” to create a new risk assessment, including a new SPRS assessment scores.



The ACRMS™ system can be manually updated at will. This provides an audit record. The system can also be auto-updated on a periodic basis to provide an auditable record of changes in compliance status. The auto-update feature is typically used after the network achieves full 110 point DFARS compliance. Weekly updates provide a convenient audit trail.

The weekly reminder email for the compliance Officer might read

Dear BLW Compliance Officer;

This is your weekly reminder to update your system status for AU-9(4), CA-7, SI-3, AU-7, AU-6, CA-2, AC-22, PE-6, and SI-2. Your SPRS score for last week was xx, compared to XX the previous week. As provided in your NDA, a copy of this email has been provided to your Apex Accelerator contact (Name here).

Regards;
Your ACR 2 Support Team

Discussion of Audit Trail and AA/MEP Supervision:

The table at right shows a typical set of monthly assessment scores for a site achieving 110-point DFARS compliance scores over a seven-month period. Manual assessments are run after installation or implementation of necessary DFARS cybersecurity controls.

Date	10/26/2022	12/26/2022	1/26/2023	2/26/2023	3/26/2023	4/26/2023	5/26/2023
Risk	GO!	GO!	GO!	GO!	GO!	GO!	GO!
E1	1	1	1	1	1	1	1
E2	1	1	1	1	1	1	1
E3	1	1	1	1	1	1	1
E4	1	1	1	1	1	1	1
E5	1	1	1	1	1	1	1
E6	1	1	1	1	1	1	1
HE1	25	25	5	5	1	1	1
HE2	25	25	5	5	1	1	1
HE3	25	25	5	5	1	1	1
HE4	25	25	5	5	1	1	1
HE5	25	5	5	5	1	1	1
HE6	5	5	5	5	1	1	1
HE7	25	5	5	5	1	1	1
HE8	25	5	5	5	1	1	1
MI1	5	5	1	1	1	1	1
MI2	5	5	1	1	1	1	1
MI3	5	5	1	1	1	1	1
MI4	5	5	1	1	1	1	1
MI5	5	5	1	1	1	1	1
MI6	50	25	25	5	5	1	1
MI7	25	5	5	1	1	1	1
MI8	25	5	5	1	1	1	1
MO1	25	1	1	1	1	1	1
MO2	25	1	1	1	1	1	1
MO3	25	1	1	1	1	1	1
MO4	25	1	1	1	1	1	1
MO5	25	1	1	1	1	1	1
MO6	50	1	1	1	1	1	1
MO7	100	5	1	1	1	1	1
MO8	50	5	5	5	1	1	1
DS	-61	-37	1	31	53	99	110

The color coded numbers are the output from an automated NIST 800-30 risk assessment. Risks to protected information are Divided into Environmental risks (E), Human Error (HE), Malicious Insider (MI) and Malicious Outsider (MO).

Risks are scored from 1 (low) to 100 (high). The red/yellow/green color coding was added to the report tables at client request about 15 years ago. The DoD Assessment (DS) scores are at the bottom of the report table.

The weekly auto assessments after achievement of full 100-point compliance allow Compliance Officers, Apex Accelerator consultants, Prime Contractors, MEP consultants, and other authorized parties to confirm ongoing DFARS compliance.

Clicking on the “GO!” button at the top of the summary column brings up the status of all the DFARS controls, as shown at right. This helps track down the causes of any deterioration in DFARS scores.

NIST Security

SG	SR	SG	SR	SG	SR	SG	SR	SG	SR	SG	SR
AC-2	Yes	AU-2	Yes	CM-5	Yes	IR-6	Yes	PE-5	Yes	SC-8	No
AC-3	Yes	AU-3	Yes	CM-6	Yes	IR-7	Yes	PE-6	Yes	SC-10	No
AC-4	No	AU-5	No	CM-7	Yes	MA-2	Yes	PE-17	NA	SC-12	Yes
AC-5	Yes	AU-6	No	CM-8	Yes	MA-3	Yes	PL-2	Yes	SC-13	Yes
AC-6	Partial	AU-7	No	CM-11	Yes	MA-4	Yes	PM-9	Yes	SC-15	Yes
AC-7	Yes	AU-8	No	CP-9	Yes	MA-5	Yes	PM-16	Yes	SC-18	Yes
AC-8	NA	AU-9	Yes	IA-2	No	MP-2	Yes	PS-3	Yes	SC-19	NA
AC-11	Yes	AU-11	Yes	IA-3	Yes	MP-3	Yes	PS-4	Yes	SC-20	Yes
AC-12	Yes	AU-12	Yes	IA-4	Yes	MP-4	Yes	PS-5	Yes	SC-23	Yes
AC-17	Partial	CA-2	Yes	IA-5	Yes	MP-5	Yes	RA-3	Yes	SC-28	Yes
AC-18	Yes	CA-5	Yes	IA-6	Yes	MP-6	Yes	RA-5	Yes	SI-2	Yes
AC-19	Yes	CA-7	No	IR-2	Yes	MP-7	Yes	SA-8	Yes	SI-3	Yes
AC-20	Yes	CM-2	Yes	IR-3	Yes	PE-2	Yes	SC-2	Yes	SI-4	Yes
AC-22	Yes	CM-3	Yes	IR-4	Yes	PE-3	Yes	SC-4	Yes	SI-5	Yes
AT-2	Yes	CM-4	Yes	IR-5	Yes	PE-4	Yes	SC-7	No	SI-8	Yes
AT-3	Yes										

DFARS cybersecurity risk assessments are listed under CUI 3.11.1. The NIST 800-171 listing refers to NIST 800-53 safeguard RA-3. RA-3 in turn references the NIST Special Publication 800-30.

Update Monthly: There are three monthly tasks and memos as shown on the following page.

NIST Safeguard	Assignee	Documents	Task Description
CM-03 CONFIGURATION CHANGE CONTROL	Compliance Officer	CUI 3.4.3 CM3 moyr.pdf	Proposed configuration changes shall be reviewed <monthly> by the <Compliance Officer>. File Configuration change proposal in Document Management Center.
AU-6(3) AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES	IT Manager	CUI 3.3.5 AU6(3) moyr.pdf	On a <monthly> basis <Compliance Officer> creates a summary report that addresses the audit log and its implications for all three tiers of risk management (i.e., organizational, mission/business process, and information system). The impact report is uploaded into the <Document Management Center>.
AC-06(9) LEAST PRIVILEGE | LOG USE OF PRIVILEGED FUNCTIONS	IT Manager	CUI 3.1.7 AC6(9) 6(10) moyr.pdf	Privileged functions shall be logged and audited on a monthly basis by the <IT Manager>. An audit memo shall be filed in the Document Management Center.

Once a month the Compliance Officer will log in to the ACRMS™ site and upload memos on proposed configuration changes and a privileged function audit report.

After the uploads the Compliance Officer shall update AU-6(3), CM-3 and AC-6(9), all of which would otherwise revert to “No”. Submit and finalize answers to create a new risk assessment and SPRS score for documentation.

Update Quarterly: The 10 quarterly tasks add up to a massive 66 points. The tasks are listed on the following page.

NIST Safeguard	Assignee	Documents	Task Description
CM-02 BASELINE CONFIGURATION	IT Manager	CUI 3.4.1 3.4.2 CM2 CM6 CM8 CM8(1) 0820.pdf	The baseline configuration of each satellite location shall be confirmed using <quarterly> network scans using the <Lansweeper vulnerability scanner>.
CM-05 ACCESS RESTRICTIONS FOR CHANGE	IT Manager	CUI 3.4.5 CM5 moyr.pdf	The <IT Manager> shall prepare an access-activities report for the <Compliance Officer> for review <quarterly>. The report will be filed in the Document Management Center.
RA-5 VULNERABILITY SCANNING	IT Manager	CUI 3.11.2 RA5 5(5) moyr.pdf	The organization scans for vulnerabilities in the information system <quarterly> and when significant new vulnerabilities potentially affecting the system are identified and reported.
CM-02 BASELINE CONFIGURATION	IT Consultant	CUI 3.4.1 3.4.2 CM2 CM6 CM8 CM8(1) 0820.pdf	The baseline configuration shall be confirmed using periodic network scans using the <Rapid Fire Network Detective> vulnerability scanner.
CA-5 PLAN OF ACTION AND MILESTONES	Compliance Officer	CUI 3.12.1 3.12.2 3.12.3 3.12.4 CA2 5 7 PL2 moyr.pdf	<Organization Name> updates existing plan of action and milestones <quarterly> based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
PL-2 SYSTEM SECURITY PLAN	Compliance Officer	CUI 3.12.1 3.12.2 3.12.3 3.12.4 CA2 5 7 PL2 0820.pdf	<Organization Name> assesses all NIST 800-171 security controls and control enhancements using the <ACR 2 Risk Management software>. See the System Security Plan Worksheet.
RA-3 RISK ASSESSMENT	Compliance Officer	CUI 3.11.1 RA3 PM9 moyr.pdf	<Organization Name> shall use the <ACR 2 ACRMS™ program or your method here> to evaluate risk at the information system level on a <quarterly> basis.
SI-3 MALICIOUS CODE PROTECTION	Compliance Officer	CUI 3.14.1 3.14.2 3.14.3 SI2 3 5 PM16 moyr.pdf	Perform periodic scans of the information system <quarterly>.
SI-4 INTRUSION DETECTION TOOLS AND TECHNIQUES	Compliance Officer	CUI 3.14.6 SI4 SI4(4) moyr.pdf	Monitoring results will be used to recalculate information security risk scores on a <quarterly> basis.
RA-5 VULNERABILITY SCANNING	Compliance Officer	CUI 3.11.2 RA5 5(5) moyr.pdf	Vulnerability remediation will be prioritized based on the results of <quarterly> information system risk assessments.

Taking the tasks individually gives the following list.

1. The baseline configuration of each satellite location shall be confirmed using <quarterly> network scans using the <Lansweeper vulnerability scanner>. The <IT Manager> will file the scan report in the ACRMS™ Document Management Center.
2. The <IT Manager> shall prepare an access-activities report for the <Compliance Officer> for review <quarterly>. The report will be filed in the Document Management Center.
3. The organization scans for vulnerabilities in the information system <quarterly> and when significant new vulnerabilities potentially affecting the system are identified and reported. The <IT Manager> will file the vulnerability scan report in the ACRMS™ Document Management Center.

4. Vulnerability remediation will be prioritized based on the results of <quarterly> information system risk assessments.
5. The baseline network configuration shall be confirmed using periodic network scans using the <Rapid Fire Network Detective> vulnerability scanner. The <IT Manager> will file the scan report in the ACRMS™ Document Management Center.
6. <Organization Name> updates existing plan of action and milestones <quarterly> based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. The <Compliance Officer> will file the updated POAM report in the ACRMS™ Document Management Center.
7. <Organization Name> assesses all NIST 800-171 security controls and control enhancements using the <ACR 2 Risk Management software>. See the System Security Plan Worksheet. The <Compliance Officer> will file the updated System Security Plan in the ACRMS™ Document Management Center.
8. <Organization Name> shall use the <ACR 2 ACRMS™ program or your method here> to evaluate risk at the information system level on a <quarterly> basis. The <Compliance Officer> shall log in to the ACRMS™ program after updating the revised safeguards and press "Submit and Finalize Answers" to create a new risk assessment, including a new SPRS assessment score.
9. Perform periodic scans of the information system <quarterly>.. See report from item 4 above.
10. Monitoring results will be used to recalculate information security risk scores on a <quarterly> basis. Follow the protocol contained in the SSP update instructions and file a copy of the assessment in the Document management center.

After collecting the necessary reports, the Compliance Officer will update the status of CM-2, CM-5, RA-5, CA-5, PL-2, SI-3, AND SI-4. The Compliance Officer can then Finalize and Update the safeguards status, generating a new SPRS score for audit.

Working with a Manufacturing Extension Partnership (MEP) or Apex Accelerator (AA): The National Institute for Standards and Technology (NIST) has created cybersecurity standards and solutions for American enterprises. The NIST Manufacturing Extension Partnership (MEP) program is a public-private partnership providing subsidized technical support services to American manufacturers. The Federal government covers half of the costs for a project. The remaining costs are split between state/local governments and client fees.

MEP offices are available in all 50 states and Puerto Rico. A Spanish language video discussing rapid DFARS cybersecurity compliance was jointly developed by ACR 2 Solutions and the Puerto Rico MEP, PRiMEX. MEPs are an excellent source of support for businesses that are increasingly dependent on rapidly changing technologies.

The DoD Apex Accelerators (AAs) were formerly known as Procurement Technical Assistance Centers (PTACs). In December 2022 PTACs were moved from the Defense Logistics Agency (DLA) to the DoD Office of Small Business Programs (OSBP). This reflects the DoD intent to increasingly focus on the small business fraction of the Defense Industrial Base (DIB).

In 2021 AA centers provided no-cost assistance to more than 56,000 organizations. AA centers are focused on helping contractors compete for federal, state, and local government contracts. AA centers have a particular expertise and focus on training and contract preparation.

There is a wide and constantly changing menu of federal, state, and local business support programs. For organizations wishing to be part of the Defense Industrial Base (DIB) a good place to start is to seek out your local AA. Their services are delivered at no cost to their clients, and they tend to have good contacts in other support organizations. An interactive map of AA centers is available here.

ACRMS™ Discounts for MEP/AA Clients: ACR 2 Solutions strongly encourages their clients to develop and maintain relationships with their local AA or ME or both. For that reason, ACR 2 offers significant discounts available only to MEP and AA clients.

As shown in the ACRMS™ order form excerpt below, the lowest prices are reserved for active AA or MEP clients, with slightly higher prices for organizations willing to become AA or MEP clients. The highest prices are reserved for the rare contractors who refuse to deal with an AA or MEP. These are also the most expensive clients for ACR 2 Solutions to support.

For Contractors who are already working with NIST Manufacturing Extension Partnerships or DoD Apex Accelerators				
0	MEP/AA-CUI Startup - 1 Site 1to50- 1 Month	MEP/AA CUI client - ACRMS DFARS 252.204-7012 Initial Compliance package - Video Boot Camp augmented Policy package, SSP creation, POAM, implementation and maintenance Task Management setup and scheduling - End with DOD Assessment score- 1 month license- credit card or check. Discounted price requires NDA permissions for an NIST MEP or DoD Apex Accelerator.	$ 495.00	$ -
0	MEP/AA -CUI-Ongoing Support-1to50-1month	MEP/AA CUI contractor version: ACRMS Ongoing Policy, SSP & POAM Updating, Task Management System, Updates and Technical Support - month by month license - credit card only. Discounted price requires NDA permissions for an NIST MEP or DoD Apex Accelerator.	$ 50.00	$ -
For Contractors who need help arranging relationships with NIST Manufacturing Extension Partnerships or DoD Apex Accelerators				
0	MEP/AA -CUI-Startup with Initial Negotiations technical support	DFARS 252.204-7012 Initial Compliance package with MEP/AA negotiations technical support. Video Boot Camp augmented Policy package, SSP creation, POAM, implementation and maintenance Task Management setup and scheduling - End with DOD Assessment score- 1 month license- credit card or check. Requires NDA and willingness to work with an NIST MEP or DoD Apex Accelerator.	$ 595.00	$ -
0	MEP/AA -CUI-Ongoing Support-1to50-1month	MEP/AA CUI contractor version: ACRMS Ongoing Policy, SSP & POAM Updating, Task Management System, Updates and Technical Support - month by month license - credit card only. Discounted price requires NDA permissions for an NIST MEP or DoD Apex Accelerator.	$ 50.00	$ -
For Contractors who do not wish to work with NIST Manufacturing Extension Partnerships or DoD Apex Accelerators				
0	CUI- Startup - 1 Site 1to50- 1 Month	ACRMS DFARS 252.204-7012 Initial Compliance package - Video Boot Camp augmented Policy package, SSP creation, POAM, implementation and maintenance Task Management setup and scheduling - End with DOD Assessment score- 1 month license - requires NDA. Credit card or check.	$ 995.00	$ -
0	ACRMS-CUI-Ongoing Support-1to50-1month	ACRMS subcontractor version: ACRMS Ongoing Policy, SSP & POAM Updating, Task Management System, updates and Technical Support - month by month license - credit card only.	$ 75.00	$ -

A complete copy of the Order Form is available on our website as document 3.

Contractual Issues and Options: Contracting issues with MEP and AA organizations are pretty straightforward for state and local small businesses. Typically the project begins with browsing to the CUI Cybersecurity page at https://cuicybersecuritycompliance.com/documents and downloading documents 1 (DFARS Cybersecurity Overview), 2 (Mutual Non-Disclosure Form or NDA), and 3 (ACRMS™ Order Form).

The NDA provides legal protection for the client and allows the client to direct ACR 2 to share the client's cybersecurity status with a MEP, AA, Prime Contractor or other key parties, as shown below.

Cyber Security Status Monitoring Permissions

Organization Name	Contact Name	Contact E-mail	Contact Phone#	Date
1. _____	_____	_____	_____	____
MEP/AA? (Y/N) ___	Confirmed? (Y/N)____			
2. _____	_____	_____	_____	____
3. _____	_____	_____	_____	____

Note that the NDA does NOT create a contractual relationship between ACR 2 Solutions and the AA or MEP. This is discussed in the 9 minute video "Introduction to the ACRMS™ for MEPs/AAs". Under the NDA ACR 2 Solutions provides client information to the MEP or AA as an agent of the client.

The ACRMS™ software allows near real-time monitoring of multiple sites. One ACR 2 medical client was able to use this software to manage cybersecurity risks at 103 sites across 16 states.

With the help of the Puerto Rico MEP PRiMEX, ACR 2 has prepared a four hour online training program for MEP and AA staff. This training is free to any MEP or AA staff who are supporting or planning to support ACR 2 clients.

ID	A	B	C	D	E	F	G	H	I	J
Date	10/28/22	10/07/22	09/23/22	08/19/22	07/28/22	07/05/22	11/02/22	11/02/22	11/02/22	11/02/22
Risk	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!	GO!
E1	50	50	50	50	50	50	1	1	1	50
E2	25	50	50	50	50	25	1	1	1	25
E3	25	50	50	50	50	25	1	1	1	25
E4	50	50	50	50	50	50	1	1	1	50
E5	50	50	50	50	50	50	1	1	1	50
E6	50	100	100	100	100	50	1	1	1	100
HE1	100	100	100	50	100	100	1	25	25	25
HE2	100	100	100	50	100	100	1	50	50	25
HE3	100	100	100	50	100	100	1	50	50	25
HE4	100	100	100	50	100	100	1	50	50	25
HE5	100	100	100	100	100	100	1	50	50	25
HE6	25	25	50	25	50	25	1	1	1	25
HE7	100	100	100	100	100	100	1	25	25	25
HE8	50	50	100	50	100	50	1	25	25	25
MI1	100	100	100	100	100	100	1	25	25	100
MI2	100	100	100	100	100	100	1	25	25	100
MI3	100	100	100	100	100	100	1	25	25	100
MI4	100	100	100	100	100	100	1	25	25	100
MI5	100	100	100	100	100	100	1	25	25	100
MI6	100	25	100	25	25	50	1	1	1	100
MI7	50	25	100	25	25	50	1	1	1	100
MI8	50	25	100	25	25	50	1	1	1	100
MO1	25	25	25	25	25	25	1	25	25	100
MO2	25	25	25	25	25	25	1	25	25	50
MO3	25	25	25	25	25	25	1	25	25	50
MO4	50	50	50	50	50	50	1	25	25	100
MO5	50	25	50	25	50	25	1	25	25	100
MO6	100	5	100	5	25	25	1	1	1	100
MO7	100	5	100	5	100	50	1	1	1	100
MO8	100	5	100	5	100	50	1	1	1	100
DS	-105	-44	-124	-39	-180	-66	110	15	15	-175