CIC Southwest 2026 - **Information Day** - block details

8:00 AM
1h 00m

Welcome & Check-in

Presentations

9:00 AM
20m

CyberAB Session - Matt Travis

The state of CMMC from the CEO of the CyberAB

9:20 AM
30m

Keynote Session

TBD

9:50 AM
1h 00m

CMMC - Start to Finish

You need CMMC to win contracts. Now the question is, what is the most cost-effective, and speedy, way to get there? This session will discuss: resources (human and monetary), and provide a multi-step plan to certification.

You will learn:

□ Briefing - CUI and the reasons why CMMC exists

□ What is a POA&M?

□ What is an SSP?

□ What level of detail is required in my evidence?

□ Recent Updates to CMMC regulation

10:50 AM
30m

Coffee Break

Presentations

11:20 AM
1h 00m

The Costs Lay in the Scope

Scoping your organization's CMMC implementation. This session provides a roadmap to a cost-effective, and manageable scope. What is an enclave and why build one? Big changes require buy-in from leadership. Often organizational/culture change is the biggest cost of CMMC compliance. The session will deep-dive into scope choices and how to deliver on those choices efficiently.

You will learn:

□ How to make the scope right-sized, hint follow the CUI

☐ Enclave or not?

☐ Service Provider, Secure Repository, or do it yourself?

12:20 PM
1h 00m

Lunch

Afternoon Presentations

1:20 PM
1h 00m

Deploying and Monitoring Microsoft Compliantly

Discussion of whether and how to use GCC-High, including costs of use and of migration. Out of the box isn't compliant. What is?

In addition, the session will cover GCC-HIgh alternatives: Microsoft Commercial, GCC, Google, and CMMC purpose built repositories for CUI.

2:20 PM
1h 00m

Documentation: Key to Compliance. Key to Profitability.

The difference between operating and operating compliantly is documentation. CMMC demands that companies build policies in writing and follow them. That means keeping artifacts of proof. This session will discuss which documents are expected (so you don't overdo it), and which artifacts are needed to prove compliance. The speaker will all talk about sources of templates and the risks of AI and its confidence building, yet often false promises.

3:20 PM
30m

Coffee Break

3:50 PM
1h 00m

Supply Chain Management - The Key to Winning Contracts in 2026

Flowdown can be the Achilles Heel of CMMC preparation. As a contractor, you are not only responsible for your compliance, but the compliance of your subcontractors. Whether you are managing a supply chain beneath you or being managed from above, understanding your responsibilities and being able to reliably execute is key.

4:50 PM
10m

Q&A Session

After a dense afternoon information delivery an ad hoc panel of experts will convene to answer questions and preview Day 2.

Networking, Food and Fun

5:00 PM
45m

Happy Hour

6:30 PM
1h 30m

Optional Dinner at The Rustic

CIC Southwest 2026 - **Workshop Day** - block details

8:00 AM
1h 00m

Breakfast & Networking

9:00 AM
10m

Welcome to Workshop Day

Roundtable Revolution - Rotation #1

Pick Your Topic and do a Deep Dive with your Peers and an Expert Facilitator -Room 1

9:10 AM
50m

CMMC Acceleration Tips and Tricks

Explore FIPS, Virtual Desktops, Secure Repositories and more...

Pick Your Topic and do a Deep Dive with your Peers and an Expert Facilitator -Room 2

9:10 AM
50m

Ask a Lawyer - False Claims, Whistleblowers and all of the Risks

This presentation provides a practical legal overview of how the False Claims Act applies to defense contractors, with a focus on whistleblower activity and enforcement trends. Attendees will gain insight into common risk areas, how investigations unfold, and strategies for minimizing exposure before issues escalate.

Key topics include:

- Overview of the False Claims Act and its application to defense contracting
- Whistleblower (qui tam) actions: how they start and why they succeed
- Common compliance failures that trigger FCA liability
- Government investigation and enforcement processes
- Financial, legal, and reputational risks for contractors
- Best practices for internal controls, reporting, and risk mitigation

Pick Your Topic and do a Deep Dive with your Peers and an Expert Facilitator -Room 3

9:10 AM
50m

Managing (and documenting) Cloud Service Providers: Yours, Mine and Ours

This presentation explains the role of the Customer Responsibility Matrix (CRM) in meeting NIST SP 800-171 requirements, clarifying how compliance responsibilities are divided between an organization and its service providers. Attendees will learn how shared responsibility works in practice, including how to validate whether a service provider has fully or partially assumed responsibility for specific security controls.

Key topics include:

- Overview of NIST SP 800-171 and third-party responsibility models
- What a Customer Responsibility Matrix is and why it matters
- Defining customer vs. service provider responsibilities for 800-171 controls
- When and how a provider may assume full or partial control responsibility
- How to validate and assess a service provider’s CRM and supporting evidence
- Maintaining alignment through contracts, SLAs, and ongoing oversight

Pick Your Topic and do a Deep Dive with your Peers and an Expert Facilitator -Room 4

9:10 AM
50m

GCC High or Not? Plus alternatives.

Many organizations operate under the mistaken belief that GCC High is the only compliant option for storing, processing, and transmitting Controlled Unclassified Information (CUI). This session explains why that is not the case, explores other compliant solutions—such as secure storage services (Dropbox , secure collaboration platforms, and Google Workspace—and helps attendees determine when GCC High is the best fit versus when alternative solutions may better meet operational and business needs.

Key topics include:

- Common misconceptions about GCC High and CUI compliance
- Actual requirements for storing, processing, and transmitting CUI
- Why GCC High is often chosen—and when it truly adds value
- Compliant alternatives to GCC High, including secure storage and collaboration tools
- Using platforms like Google Workspace to meet CUI requirements
- Matching solutions to use cases, risk tolerance, and business needs

Pick Your Topic and do a Deep Dive with your Peers and an Expert Facilitator -Room 5

9:10 AM
50m

Choosing a Service Provider (Implementation, Security Services, and Assessments)

This session explores the benefits of engaging third-party service providers such as RPOs, C3PAOs, and MSPs, while highlighting the critical need for due diligence—not all providers are equally qualified or able to deliver on their claims. Attendees will learn how to evaluate, select, and manage service providers effectively to reduce risk and ensure long-term compliance and operational success.

Key topics include:

- Roles and differences between RPOs, C3PAOs, and MSPs
- Benefits and risks of relying on third-party service providers
- Common red flags and misleading claims to watch for
- Key questions to ask when evaluating a service provider
- How to verify qualifications, experience, and scope of services
- Best practices for managing and governing ongoing provider relationships

Pick Your Topic and do a Deep Dive with your Peers and an Expert Facilitator -Room 6

9:10 AM
50m

Artifacts and Evidence - Creating Proof of Process

This session explains why CMMC compliance goes beyond written policies and procedures to require clear, defensible artifacts and evidence that demonstrate controls are implemented, operating as intended, and effective. Attendees will learn how to create, maintain, and curate proof of process over time—because in CMMC, if it isn't documented and supported by evidence, it effectively doesn't exist.

Key topics include:

- The role of artifacts and evidence in CMMC assessments
- Difference between documentation, implementation, and operational proof
- What assessors look for as valid and sufficient evidence
- How to create, maintain, and curate artifacts over time
- Mapping artifacts to CMMC practices and processes
- How GRC platforms can simplify evidence collection, organization, and maintenance

Pick Your Topic and do a Deep Dive with your Peers and an Expert Facilitator -Room 7

9:10 AM
50m

AI and CMMC - Uses and Perils (and Security!)

Compliance implications for using AI on top of the dealing with tools that may only be 70% accurate, or could leak your data if not configured properly. During this roundtable contractors share approaches to managing AI tool proliferation while protecting CUI and maintaining CMMC compliance.

- Discovery and inventory: finding AI tools already in use across the organization
- Risk assessment: data exposure, model training, and third-party processing
- Policy development: acceptable use, data handling, and approval processes
- Technical controls: DLP integration, network monitoring, and access restrictions

- Vendor management: AI service provider assessments and contract terms
- Training and awareness: helping employees understand AI risks and proper usage

Pick Your Topic and do a Deep Dive with your Peers and an Expert Facilitator -Room 8

9:10 AM
50m

Remediation - It is about the POA&M

Round table attendees will trade proven approaches to POA&M development that satisfy assessors and actually drive security improvements.

- Writing deficiencies that pass: root cause analysis, risk scoring, and remediation specificity
- Milestone planning: realistic timelines, resource allocation, and dependency management
- Evidence linkage: connecting findings to controls and tracking remediation proof
- Risk management: accepting, mitigating, and transferring risks appropriately
- Ongoing maintenance: tracking progress, updating timelines, and closing items
- Assessor perspective: what makes a POA&M acceptable vs. what triggers re-work

End of Pick Your Topic and do a Deep Dive with your Peers and an Expert Facilitator

10:00 AM
20m

Coffee Break

Roundtable Revolution - Rotation #2

10:20 AM
50m

Rotation 2

The second Roundtable Rotation will cover the same topics. Facilitators will remain at their tables while attendees rotate, giving each participant a deep dive into a second topic with the facilitator and their peers.

11:10 AM
20m

Coffee Break

Mock Assessment

11:30 AM
1h 00m

Advice from the Front Lines

Observe a mock assessment with a C3PAO and an OSC. What is the flow of the audit? How to stay out of trouble from over-sharing, or not having the right materials available. Just how much evidence do you need? The answers are here.

12:30 PM
15m

Lunch for Participants in the Compliance Jam™Learning Lab

Lunch will be served and participants will begin the Lunch-n-Learn where they will be able to start exercising their knowledge in a gratis FutureFeed subscription using either sample data or their own data.

Compliance Jam™Learning Lab - Scoping and Resourcing

12:45 PM
1h 00m

Group Exercise (Sponsored by FutureFeed)

We all log in together. You will use FutureFeed, a leading GRC tool (or a tool of your own) to either define and document your system (or to use sample data to practice the process). In this session, we'll help you organize much of what is likely already in your head to ready as evidence the CMMC controls.

Compliance Jam™Learning Lab - Assessing Controls

1:45 PM
1h 00m

Group Exercise (Sponsored by FutureFeed)

After a break, we'll go through a few controls, using the sample evidence and an expert RPO to associate and document specific controls. You'll walk through a process of gathering evidence and artifacts, and then tying them together with objective statements and summary notes.

2:45 PM
10m

Reflections & Feedback Poll