CMMC 101

Washington APEX Accelerator

Presenter: Cara Buckingham

February 3, 2026

This APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense

About the Presenter

Cara Buckingham is the Center Manager and Advisor for Washington APEX Accelerator at Economic Alliance of Snohomish County.

Prior to APEX, Cara worked in the construction industry where she helped build relationships with buyers and tracked small business programs to pursue government contracts. Buckingham served as a member of both the AGC of Washington (AGC) Diversity and Inclusion Committee and the Washington State Business Diversity Advisory Group to improve small business access to state procurement. She currently serves on the AGC of WA Board of Trustees.

Other past professional lives include marketing and PR for the shopping center industry and working as a radio and television journalist. As a communications professional, she enjoys connecting people and resources to help them meet their business goals.

1 Kitsap Economic Development Alliance
Mary Jo Juarez, Terry Homburg, James Davis

2 Thurston Economic Development Council
Grady Smith

3 Columbia River Economic Development Council

4 Economic Alliance Snohomish County
Cara Buckingham, Mark Johnson

5 Green River College
Darrell Sundell, Melinda Martirosian

6 Washington APEX Accelerator in Pierce County
Trena Payton, Maryam Lynch-Tate

7 Greater Spokane Incorporated
Aleesha Roedel

8 Tri-City Regional Chamber of Commerce
Maria Alleman

Other APEX Accelerators Serving Washington State

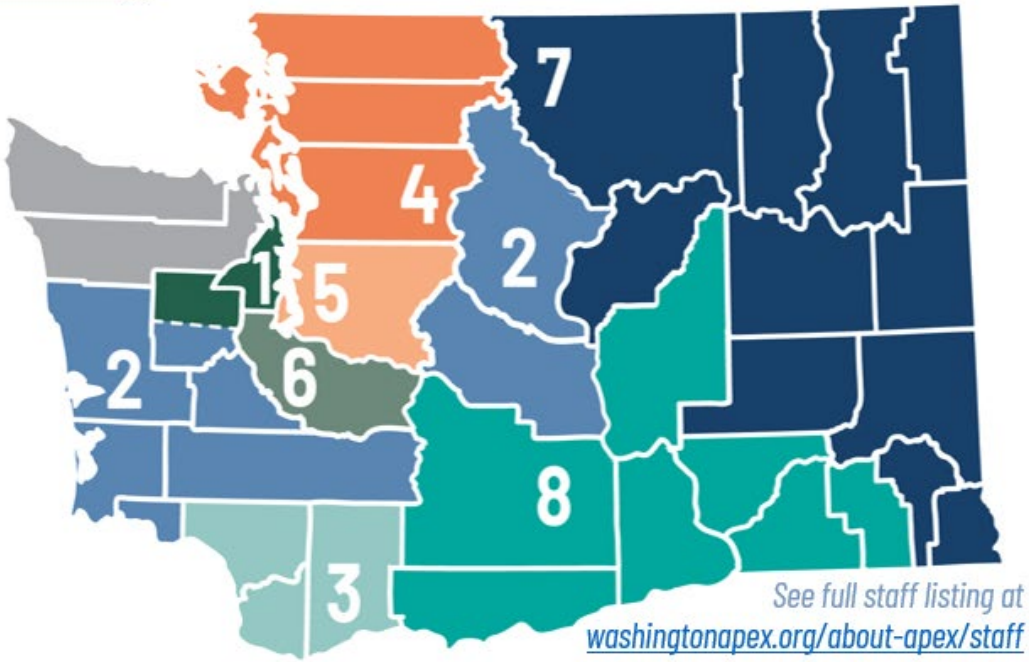
North Olympic Peninsula APEX Accelerator: clallam.org/apex

American Indian Chamber Education Fund APEX Accelerator: aicef-apex.org

NW Native Apex Accelerator: nnapex.org

Innovation & SBIR Program
washingtonapex.org/sbir

WASHINGTON APEX ACCELERATOR



See full staff listing at
washingtonapex.org/about-apex/staff

360.860.6945 info@washingtonapex.org washingtonapex.org

"This APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense."

WASHINGTON APEX ACCELERATOR
Economic Alliance SNOHOMISH COUNTY

Sponsors and Supporters

DES

Washington State
DEPARTMENT OF
ENTERPRISE SERVICES

Port of Seattle®

Aprio®

City of Seattle

WASHINGTON APEX ACCELERATOR

Economic Alliance SNOHOMISH COUNTY

What is CMMC?

- CMMC = Cybersecurity Maturity Model Certification
- Department of Defense
- Sets cybersecurity standards for contractors and subcontractors doing business with the DoD on how to properly handle ‘protected information’

What is Protected Information

- Federal Contract Information (FCI) – any information flowing in and out of a business related to a DoD contract EXCEPT invoices
- Controlled Unclassified Information (CUI or CDI) – sensitive government information including technical drawings, blueprints, export-controlled data, etc.

Why does CMMC exist?

- Defense contractors have been targeted by cyberattacks.
- The DoD needed a way to **verify** that companies are following cybersecurity rules (not just promising they do).
- CMMC provides a framework with **tiers of cybersecurity requirements**, aligned with NIST 800-171 standards.

Who Does CMMC Apply to?

All primes, subcontractors and suppliers contracting with the Department of Defense **excluding**...

- Businesses selling Commercially Off the Shelf Items (COTS) **without modifications**
- Contracts under the micro-purchase threshold of $15k

What is the Framework?

Level 1 – Foundational

- Basic cybersecurity practices (like antivirus, firewalls, secure passwords).
- Applies to contractors that only handle **FCI**.
- Requires an annual **self-assessment**.

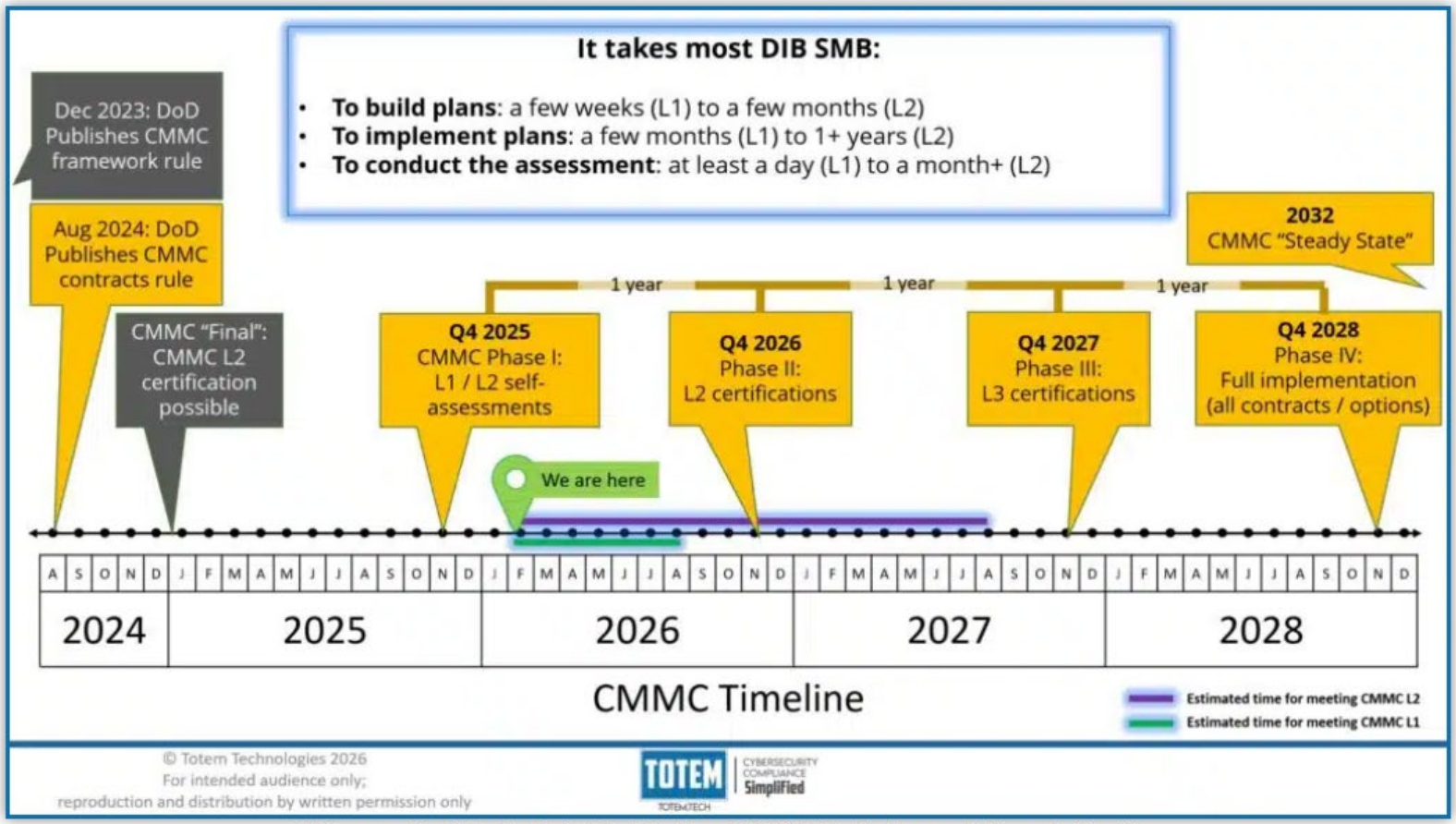
Level 2 – Advanced

- Based on **NIST SP 800-171** (110 security requirements).
- Applies to contractors handling **CUI**.
- Requires either **self-assessment** or **third-party certification**, depending on the sensitivity of the work.

Level 3 – Expert

- Based on **NIST SP 800-172** (enhanced practices).
- Applies to the most sensitive programs.
- Requires a **government-led assessment**.

Implementation Timeline?



Cybersecurity Maturity Model Certification (CMMC) Finalization and Phase-In Timeline

Challenges for Businesses

- Many Small and Medium Size Businesses handling Federal Contract Information (FCI) don't know where to begin with cybersecurity compliance

- FAR 52.204-21 requirements are complex

- Limited time and resources make it difficult to build a compliant cybersecurity program

Steps to Becoming CMMC Level 1 Compliant

Steps to Becoming CMMC Level 1 Compliant

STEP 1

- Identify whether you handle Federal Contract Information (FCI)

- If your contract includes FAR 52.204-21 or DFARS 252.204-7024, you must protect FCI

Steps to Becoming CMMC Level 1 Compliant

STEP 2 – SCOPE/INVENTORY

- Identify the systems, people & locations that store, process or transmit FCI

- Conduct a comprehensive inventory

- If possible, exclude unrelated systems to minimize compliance scope (good for small businesses)

Steps to Becoming CMMC Level 1 Compliant

STEP 3 – FAR 17 Controls Self-Assessment

- Understand the controls need to meet

Steps to Becoming CMMC Level 1 Compliant

Control Categories

Domain	Example Practices
Access Control (AC)	Limit access to authorized users; control use of removable media.
Identification & Authentication (IA)	Require unique user IDs and strong passwords.
Media Protection (MP)	Properly sanitize or destroy FCI media before disposal.
Physical Protection (PE)	Limit physical access to systems and devices.
System & Communications Protection (SC)	Protect information during transmission; maintain secure connections.
System Integrity (SI)	Update software, patch systems, and protect from malware.

Steps to Becoming CMMC Level 1 Compliant

STEP 4 – Document Policies and Procedures

- Describe how your company will meet all controls by creating a System Security Plan (SSP)
  - Who responsible for security
  - How implementing each practice
  - Screenshots, logs, and system settings

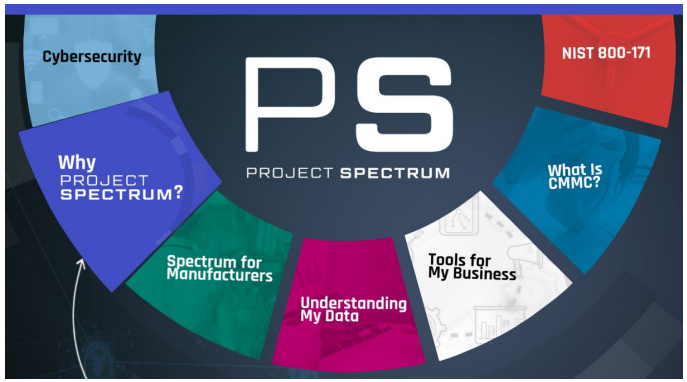
Steps to Becoming CMMC Level 1 Compliant

STEP 5 – Perform Self Assessment/Submit Results

- Submit into Supplier Performance Risk System (SPRS)
- There is no "score" for CMMC Level 1 Self Assessment
- Must meet all controls or safeguards at 100%
- This must be reported annually

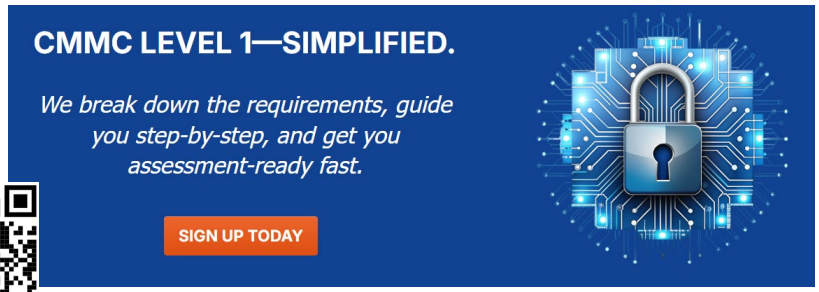
Resources to Help with CMMC Level 1 Compliance

DOD's Project Spectrum offers free tools for gap analysis



APEX Accelerator offering a CMMC Level 1 Readiness Workshop Series

- Sessions offered in January, February, & March 2026



WASHINGTON APEX ACCELERATOR
Economic Alliance SNOHOMISH COUNTY

CMMC Level 1
Workshop Series

- Partnership: Washington APEX + Totem.Tech + Govology

- Short, hands-on online workshops

- Target audience: SMBs in the Government Industrial Base (GIB) & Defense Industrial Base (DIB)

What You'll Learn

Session	Theme	Topic
1	Overview of Requirements and Scoping	Overview of Federal Government / CMMC cybersecurity compliance System Inventory basics System Description workbook introduction
2	Building an SSP	Principles of quality cybersecurity policies Addressing the FAR 17
3	Self-Assessment	The DoD's 800-171 Assessment Methodology for the associated FAR 17 controls Reporting assessment results in the DoD's Supplier Performance Risk System (SPRS)

What You'll Accomplish

- Start building a System Security Plan (SSP)
- Implement protections for FCI per FAR 52.204-21
- Conduct a CMMC Level 1 self-assessment
- Become "GIB Ready" or "DIB Ready"
- Prepare for eventual CMMC Level 2 certification, if applicable

Learning Outcomes

- Understand federal contractor cybersecurity requirements

- Develop your System Security Plan (SSP) "blueprint"

- Learn DoD self-assessment and reporting methods

How It Works

- Watch On Demand Tutorials (1.5 hours each), recommended at beginning of the week

- Review additional training materials – Workbook, PowerPoints

- Attend weekly live Q&A sessions (1 hour each, Fridays), from 8am – 9am PT

What You'll Receive

- e-Workbook
- Access to Totem™ Cybersecurity Compliance Management Tool
- SSP Template & Policy Templates
- Weekly Q&A support

Get Ready for Success

- Inventory of user accounts, hardware, software

  Here is a good article by Totem Tech about that

- Totem template accessed here*

*You will see references to CUI (Controlled Unclassified Information) which is tied to CMMC Leve 2. However, you can use the template as a guide to inventory your hardware and software for CMMC Level 1 which applies to FCI (Federal Controlled Information).

Attendee Requirements

- Documentation & system details
- Workstation with Internet
- An open and curious mindset!

Instructor Contact Information

Cara Buckingham– carab@economicalliancesc.org
Washington APEX Accelerator at Economic Alliance Snohomish County

Cohort Registration Link