Compliance Consultants, Platforms, and Assessors

How to find the right fit for your company.

Current As Of: August 2024

Sponsored by:

TODAY'S SPEAKERS

Allison Giddens

Co-President

Win-Tech, Inc.

Vince Scott

CEO

Defense Cybersecurity Group

INFRAGARD DIB Sector

Sponsored by:

TODAY'S SPEAKERS

Amira Armond

Founder

Kieri Solutions

Ryan Bonner

CEO

DEFCERT

Sponsored by:

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- **Know your Contracts**
  - Your contracts should tell you what information you must protect
- **Define & Understand your business processes to identify how & where you store / handle / transmit CUI**

Sponsored by:

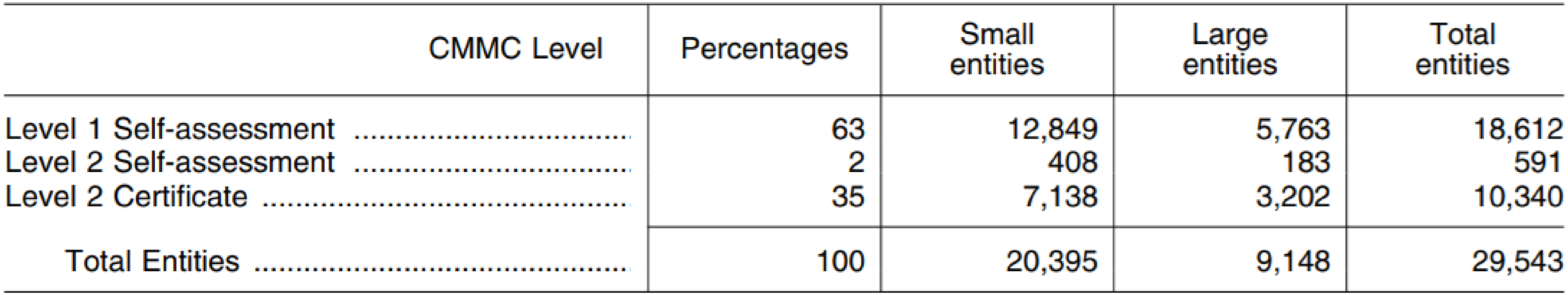
Latest news – 48CFR

- **Updates 252.204-7021**
  - Contractor shall only process, store, or transmit data on information systems that have a CMMC certificate at Level ______ or higher…
  - Notify the Contracting Officer within 72 hours if there is a lapse of security or change in certification status…
  - Ensure that subcontractors have a current CMMC certificate appropriate to level flowed down

- **Does NOT update 252.204-7012**

- **Implications of the DoD UID, SPRS, CMMC eMASS**

Latest news – 48CFR



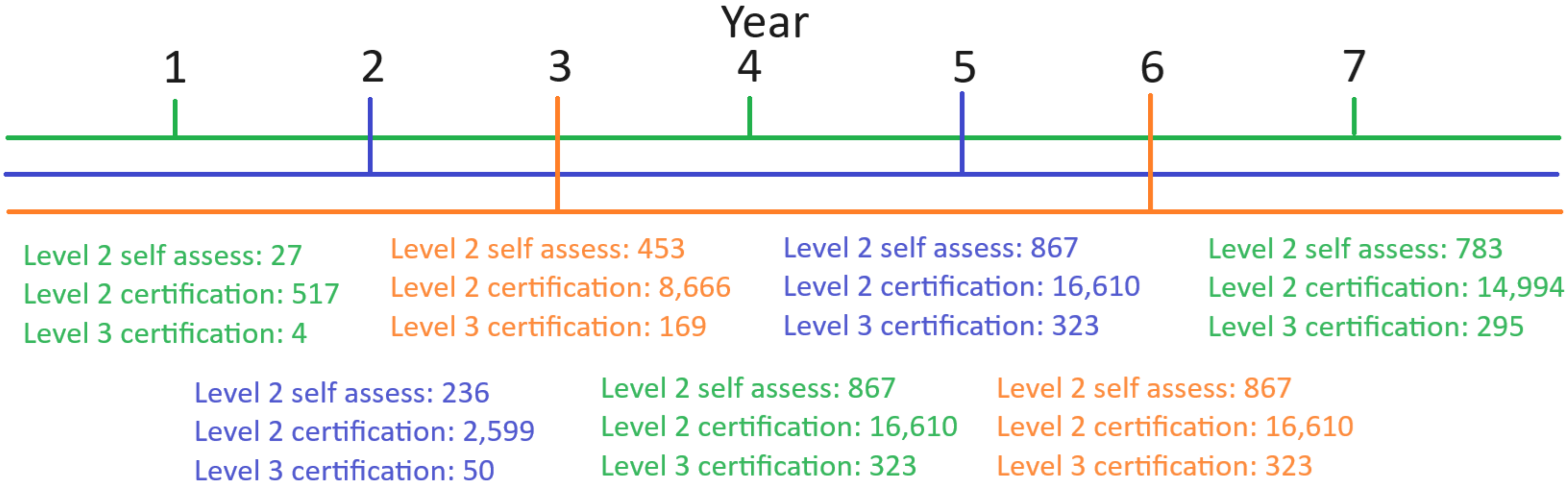
CMMC Level	Percentages	Small entities	Large entities	Total entities
Level 1 Self-assessment	63	12,849	5,763	18,612
Level 2 Self-assessment	2	408	183	591
Level 2 Certificate	35	7,138	3,202	10,340
Total Entities	100	20,395	9,148	29,543

During the first three years of the phased rollout, the CMMC requirement will be included only in certain contracts for which the CMMC Program Office directs DoD component program offices to include a CMMC requirement.

After three years, DoD component program offices will be required to include a requirement for CMMC in solicitations and contracts that will require the contractor to process, store, or transmit FCI or CUI on contractor information systems during contract performance.

- Federal Register / Vol. 89, No. 158 / Thursday, August 15, 2024 / Proposed Rules

Latest news – 48CFR



Level 2 self assess: 27
Level 2 certification: 517
Level 3 certification: 4

Level 2 self assess: 236
Level 2 certification: 2,599
Level 3 certification: 50

Level 2 self assess: 453
Level 2 certification: 8,666
Level 3 certification: 169

Level 2 self assess: 867
Level 2 certification: 16,610
Level 3 certification: 323

Level 2 self assess: 867
Level 2 certification: 16,610
Level 3 certification: 323

Level 2 self assess: 867
Level 2 certification: 16,610
Level 3 certification: 323

Level 2 self assess: 783
Level 2 certification: 14,994
Level 3 certification: 295

Sponsored by:

48CFR: Small business manufacturer perspective

1. Were you looking for clarification for the program? Because this wasn't the place to find it.

2. DoD tells us this is NOT the place problems surrounding CUI are solved. (Well, we tried.)

3. There is nothing in the rule that addresses potential accommodation or mitigation for small businesses.

Sponsored by:

48CFR: Small business manufacturer perspective

The biggest takeaway:

Prime contractors are responsible for ensuring their subcontractors meet flow-down provisions – and it'll start sooner than you think.

Use this opportunity to communicate with your customers (and vendors).

- **Pay close attention to the data you receive and create.**
- **Is your customer blindly flowing down clauses when they don't apply?**
- **What does YOUR supply chain look like and what data must you share with them?**
- **Keep your eye out for sneaky change orders.**

Stay the course and just aim to be better today than you were yesterday [on your CMMC path].

Sponsored by:

CMMC Platforms

- Types of platforms
- Not buying “one thing”
- People are the critical path
- Tools market is improving

Sponsored by:

External service providers

- **Goals**:
  - Know how your provider is **helping you** perform security requirements
  - Ensure they perform appropriate controls
  - Evaluate regularly

- FedRAMP and CMMC certifications only tell you that *their* network is secure. Need more information if they are doing requirements for *your* network.

- Due in late October: Final version of 32 CFR CMMC rule
  - Non-cloud external providers = CMMC Level 2
  - Clouds handling CUI = FedRAMP
  - Clouds handling Security Protection Data = ?? (FedRAMP likely)

Sponsored by:

How are External Service Providers assessed?

- **Currently no procedure for assessing ESPs**
  - CMMC Assessment Process in re-write

- **Assessors need to understand how requirements are performed by the ESP for *your* information system.**
  - Do they patch your servers? Need evidence
  - Do they review your audit logs? Need evidence

Customer Responsibility Matrix + CMMC Certification = evidence

Available to interview and demo during assessment = evidence

What is a Managed Services Provider (MSP)?

- Outsourced IT and security labor delivered as services
- May manage cloud infrastructure on behalf of an organization
- Most MSPs are unlikely to process, store, or transmit CU
- Common MSP responsibilities:
  - Configure and manage networks, servers, and cloud infrastructure
  - Manage day-to-day IT needs (system administration, help desk support)
  - Monitor security tools and respond to alerts and incidents

Applicable CMMC Practices for MSP

- People: training, privileged management, account requirements, background screening
- Technology: MSP will be expected to perform internal security for their systems if persistent connections exist to your network (remote management tools, VPNs)
- Facility: only if storing CUI at MSP
- Compliance activities: Change Mgmt., Incident Mgmt., maintenance, vulnerability scanning, etc.
- Assessor will need to evaluate MSP to verify any compliance activities they perform on DIB Company’s behalf

How to Select an MSP for CMMC

- Demand a Shared Responsibility Matrix (SRM) designed for use with CMMC
- Ask:
  - Does the MSP maintain remote access connections to your environment?
  - How does the MSP manage changes to your environment?
  - Does the MSP have staff qualified to act as CISO for you?
  - Are all MSP employees U.S. Persons?
  - What clouds and subcontractors does the MSP use to support you?
  - Has the MSP implemented NIST SP 800-171 for its internal systems?

Sponsored by:

Additional Resources for Vetting MSPs

- MSP Shopping Guide
  - ND-ISAC, SMB Working Group
- MSPs and CMMC Compliance
  - https://www.cmmcaudit.org/msps-and-cmmc-compliance/
- MSP Maturity Check: 21 Questions to Ask Your MSP
  - https://steelroot.us/resource/msp-cybersecurity-check/

Sponsored by:

Costs – Getting Compliant / Staying Compliant

- For small businesses, <200 employees
- Likely a 6-figure expense annually
  - Cost for 5-person company roughly = to 25-person company
- Starting from 0, technical implementation:
  - $80 - $150K if outsourcing
  - Higher if in-sourcing
- Sustainment Budget: ~$3500 - $4000 / user / per year
  - 5-person to 25-person company: $87,500 - $100,000
  - IT spend related to compliance, not all IT spend
- Economies of scale: ~100+ employees

Sponsored by:

Journey of a Small Business

- **Started in 2020**
  - Utilizing free template resources
- **2021 - 2022**
  - 2021 migrated to GCC-High after hiring 3rd party
  - Transition from “commercial” MSP to DIB specialist
- **2022 – 2023**
  - Changed network infrastructure
  - By end of 2023, buttoning up loose ends.

Lessons Learned

- **Managing competing priorities**
  - Have to ensure CMMC compliance stays at the top
- **Breaking into manageable pieces**
- **Maintaining a budget**
- **Keep improving**
  - A “little” better today – know you are on track
- **Maintaining network of subject matter experts**

Questions

Sponsored by: