securitymetrics®

The Devil's in the Details

Everything Level 1 CMMC Compliance
Requires and Nothing It Doesn't

Introductions

- **21 years** in Cybersecurity
- **10 years** as a Software Developer
- **7 years** as an Aerospace Engineer (McDonnell Douglas Space Systems)

Gary Glover

Vice President of Assessments

CISSP, CISA, QSA

Agenda

01
Getting Real: Can I Make it Through a Level 1 Self Assessment

02
Scoping: Get This Right First

03
Applying Level 1 Practices

04
Getting Help: Where to Go

05
Storing Your Compliance Evidence

06
L1 Contractors: Deepest Roots of CMMC Flow-Down

Recent Developments

- Pause in DoW validation requirements for Level 2
- Does not represent a change in Level 1 validation requirements
- Nice, you can ignore the hype
- Federal Regulations are in force, supply chain still needs protecting
- Prime contractors still need to know subcontractor compliance status, no change there in Flow-down requirements
- Don’t get stuck in “analysis paralysis” of this issue…keep going
- Level 2’s are also now firmly in Self-Assessment situation

Getting Real:

Can I Make it Through a CMMC Level 1 Self Assessment?

Where Businesses Get Stuck

- **“Surely the rules will change.”** Don’t wait for the CMMC to change. Most likely they won’t change, so start now
- **“I have not seen Self Assessment required yet**.” We are starting to see it in L1 contracts, don’t put off getting ready
- **“It’s going to be hard and expensive!”** Yes, it takes real work, but if you have tools and good support it is possible
- **“CMMC L1 is asking too much!”** The bar is basic cyber hygiene. Antivirus, strong passwords, limiting who walks in the door, etc.
- **“CMMC is not reasonable!”** It is very similar to what small businesses in other industries have been required to do for over 20 years…we work with 500,000 active customers

CMMC L1: Not New, Not Scary.

- **Familiar Compliance Experience?**
  - Complied with other cybersecurity frameworks like (SOC2, PCI DSS, CIS) this will feel familiar, same cybersecurity controls, different acronym
- **Basic Cyber Hygiene**
  - Antivirus, unique passwords, update systems, locking down who can walk in, etc.
  - It is not enterprise-grade security
- **The Bar Is Realistic**
  - Just **15** practices and **59** objectives
  - Level 2 requires **110** practices – **320** objectives

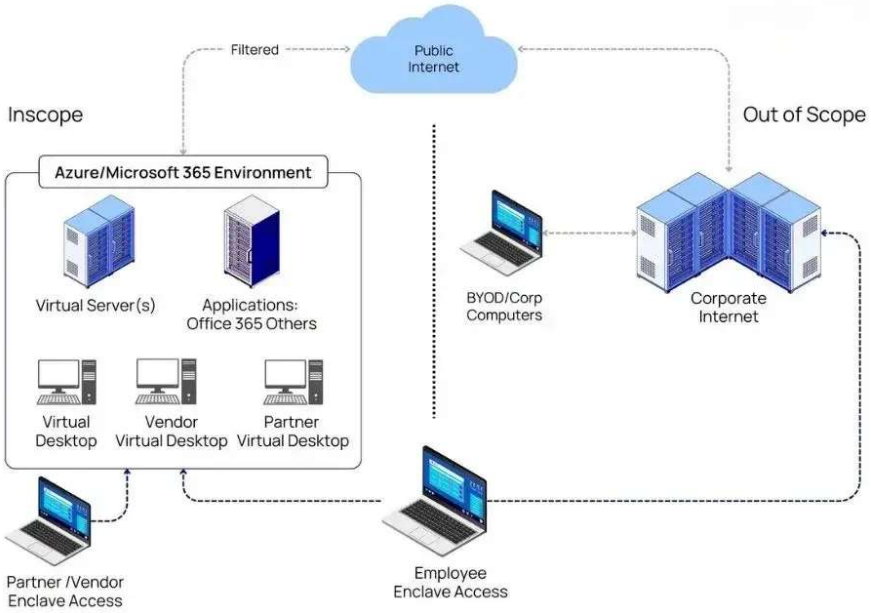
Scoping:

Get This Right First

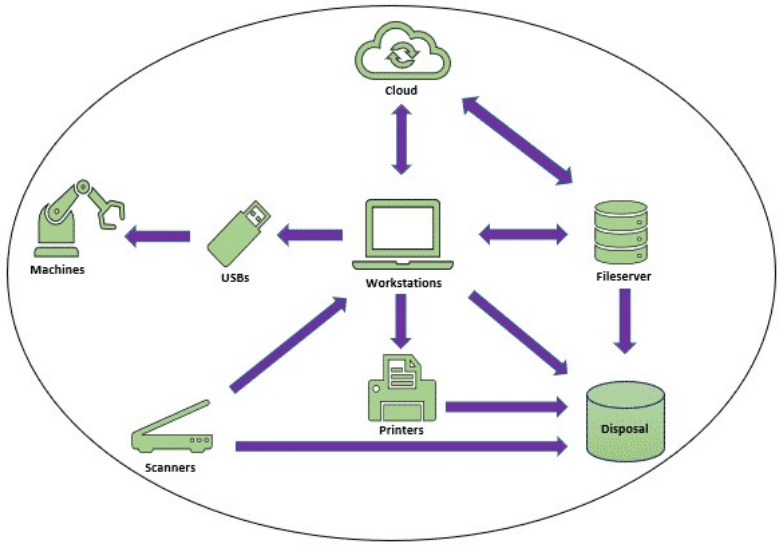
Scoping Your FCI Data Environment

- **Find the Data**
  - Clearly define and document the Federal Contract Information (FCI) you are getting
  - Research where FCI flows and where it may pool in the corners of business networks and processes
- **Minimize the Boundary**
  - Segment networks and systems so fewer machines and people ever touch FCI
- **Diagram It**
  - Simple network diagram and data flow so anyone can follow it

Network Diagram Example



Data Flow Diagram Example



Minimize Your Scope!

- **Think hard**
  - Can current business processes involving FCI be modified?
  - Ask the question: “Do I really need it there?”
- **Minimize**
  - Segment networks and systems so fewer machines and people touch FCI
  - Example: Do I need FCI access from my phone?
- **Using enclave may reduce scope**
  - Not an “easy” button but learn about current technologies being used
  - Cloud enclave, virtual access, single dedicated laptop, etc.

Applying
Level 1 Practices

Keep Calm

- **Focus on the harder requirements first.** Spend your prep time on the controls that will take more work
- **It's the right thing to do.** These are protections you should have regardless of CMMC, so give in and get it done
- **Education pays off.** Time spent understanding the requirements is never wasted
- **Read the DoW Assessment Guide.** The discussion and examples in the Level 1 Self-Assessment Guide are genuinely helpful
- **It's not one-and-done.** Reassess every year, and update sooner if your systems change
- **20 years of proof.** We've walked small businesses through frameworks like this many times, it is possible

CMMC L1 Core Security Domains

There are 6 core domains and a total of 15 practices between those domains that must be in place. Each practice has several smaller objectives

1. **Access Control (AC) – 4 practices, 19 objectives**
    - Limit access to only authorized users, doing authorized functions
    - Limit connections to and use of “external” systems
    - Don’t expose FCI on publicly accessible systems
    - Document policy and procedure to meet objectives (how to do it…)

2. **Identification and Authentication (IA) – 2 practices, 6 objectives**
    - Use unique usernames for all access to systems & networks where FCI is present
    - Authenticate all users before access is granted into systems & networks
    - Document policy and procedure to meet objectives

CMMC L1 Core Security Domains

3. Media Protection (MP) – 1 Practice, 2 objectives

- Sanitize or destroy media containing FCI (hard disk, paper, etc.) before disposing it or reusing it
- Document policy and procedure to meet objectives

4. Physical Protection (PE) – 2 practices, 10 objectives

- Limit physical access to systems and environments to only authorized individuals
- Control and manage all devices/equipment used to limit physical access
- Escort visitors, monitor activity, keep visitor log
- Document policy and procedure to meet objectives

CMMC L1 Core Security Domains

5. System and Communications Protection (SC) – 2 practices, 10 objectives

- Monitor and protect external and internal network boundaries where FCI is present
- Separate sensitive internal systems dealing with FCI from publicly accessible systems by using properly segmented network design
- Document policy and procedure to meet objectives

6. System and Information Integrity (SI) – 4 practices, 12 objectives

- Update systems and software in a timely and regular basis
- Protect systems and networks storing, processing, or transmitting FCI from malware (e.g.- use anti-virus software)
- Regularly update anti-malware software
- Perform periodic malware scans on systems, scan externally received files for malware before use or execution
- Document policy and procedure to meet objectives

Operational Notes for Level 1 Compliance

- **Self Assessment is the only validation required**
- **Must complete an annual reaffirmation in DoW SPRS system**
- **No POA&Ms are allowed**
  - All practices must be in place at time of self assessment
  - No Plan of Action or future Milestones (POA&M) allowed for any of the 15 practices

securitymetrics®

Getting Help:

Where to Go?

First Thing, What Kind of Help is Needed?

- **Questions you can ask yourself:**
  - Do I have a good grasp if CMMC requirements?
  - Do I have documented policy and procedures for FCI protection?
  - Do I know ways to lock down my network or systems?
  - Does our company have internal IT admin with cybersecurity knowhow? (If so, Delegate!)
- **Questions like these can help you determine early on what kind of help you need**
  - CMMC experts, documentation help, network architecture, etc.

Paths to Get There

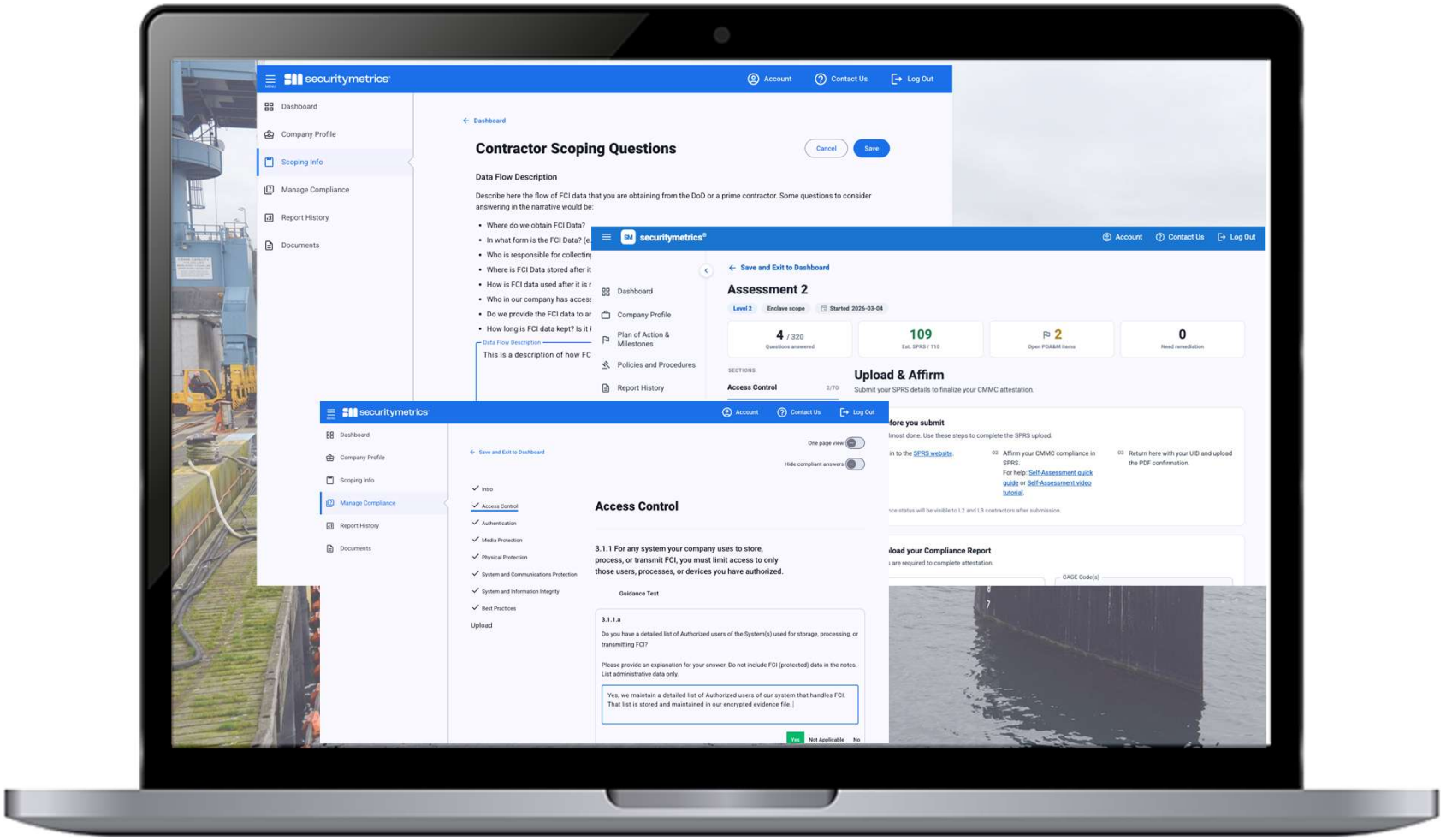
Path	What It Looks Like	Best Fit
Do-It-Yourself	Download self assessment documents, read guidance and make any necessary system and network changes	Team with lots of cybersecurity experience. Finalized policy and procedure documents, etc.
Self-Assessment Portal	Guided online tool that turns NIST SP 800-171 into plain-language questions, with templates and real support	Teams with less internal knowledge needing guided support and wanting to save time
Consultant (RPO / CCA)	Local or remote expert who knows small-business realities and can help with network, software, or documentation work	Teams that want professional help, care about reducing risk more and may need hardware implementation support
Enclave Solutions	A hardened enclave or a few dedicated laptops that shrink the FCI footprint instead of fixing the existing network	Businesses that isn't as price sensitive and wants clear isolation of scope. It can be a build or buy solution.

Level 1 Self Assessment Portal Providers

- **Some Portal Providers**
  - CMMCTrack
  - ecfirst
  - SecurityMetrics
  - Totem Technologies

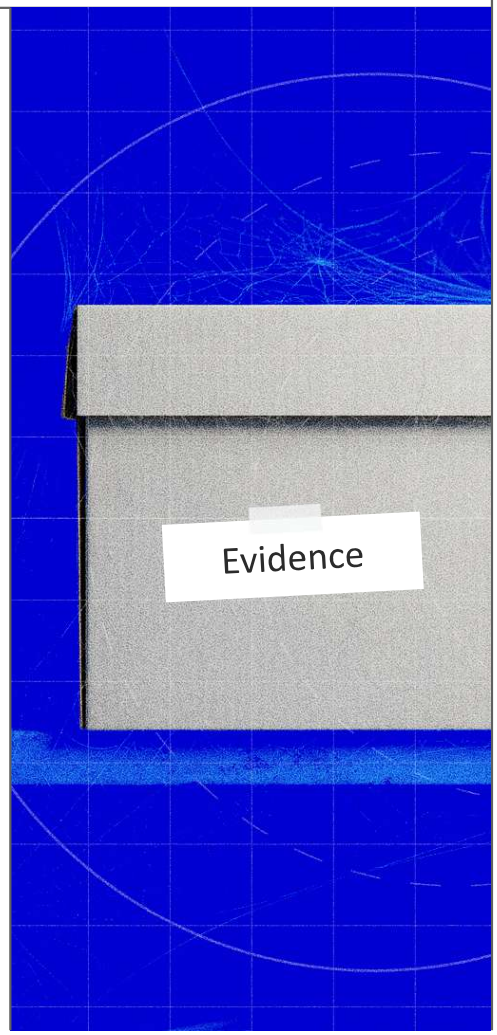
- **Portal Features to look for**
  - Simplified NIST 800-171 rev 2 language, questionnaire form
  - Online help and extra guidance information
  - Live 24/7 support with skilled technical agents, not just AI chatbot
  - Storage of SPRS validation evidence, helps with reporting to primes

Portal Example



Storing Your Compliance Evidence

- **Ways to Store It**
  - A lightweight GRC tool built for Level 1 — most vendors focus on Level 2 today, but a few are starting to help L1 entities
  - A folder of organized and dated files on a computer that can be linked to L1 CMMC requirements
  - Simple L1 SSP spreadsheet where you can document and link evidence
- **Keep It for Years**
  - Retain evidence across multiple annual cycles, not just the most recent one
- **Do It Every Year**
  - A senior official reaffirms compliance in SPRS annually, refresh your evidence on the same schedule



L1 Contractors:

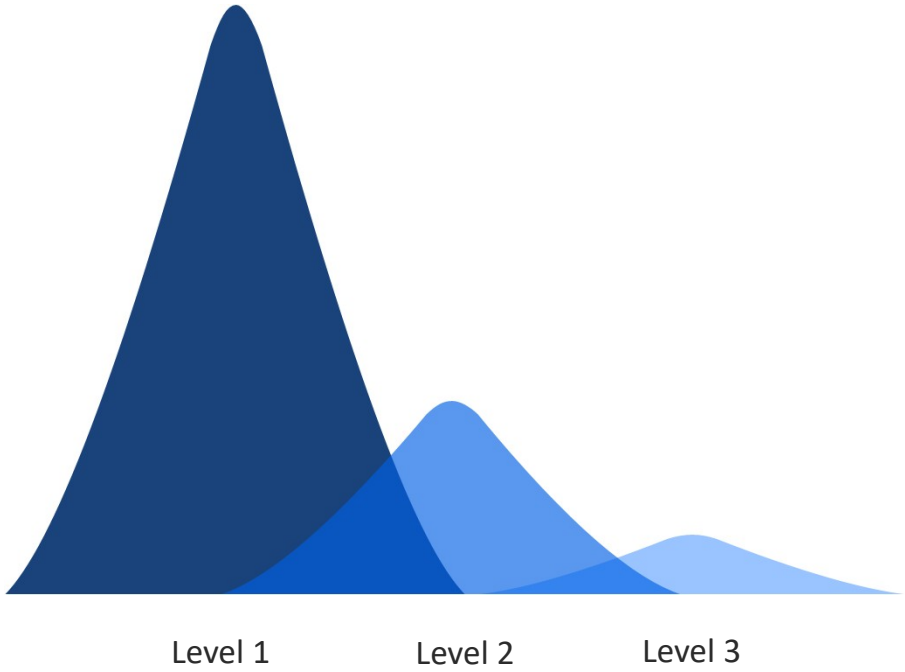
The foundation of CMMC Flow-Down

CMMC Flow-Down

"New CMMC flow-down requirements mandate that prime contractors "flow down" Cybersecurity Maturity Model Certification (CMMC) obligations to subcontractors at all tiers in the supply chain…"

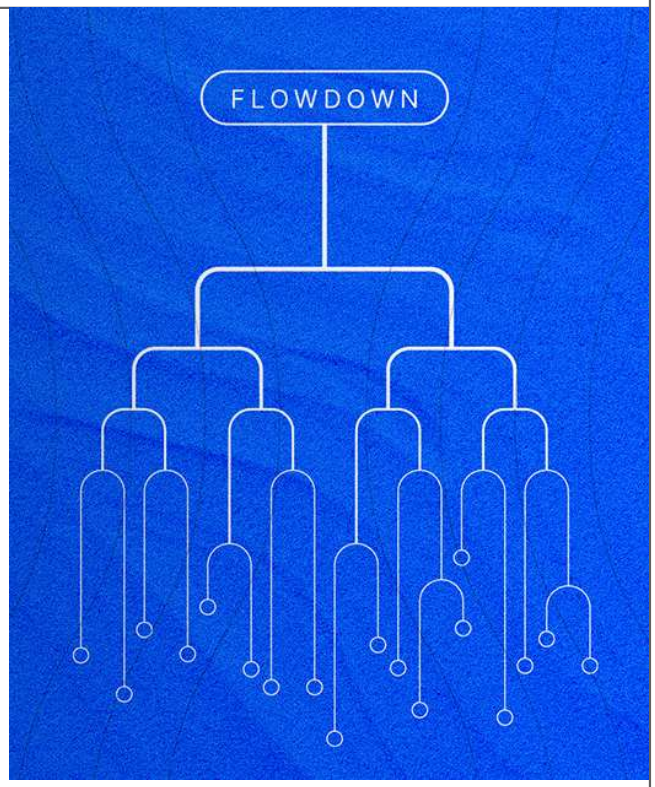
What will this look like for a L1 Subcontractor?

There is a LARGE number of L1's…

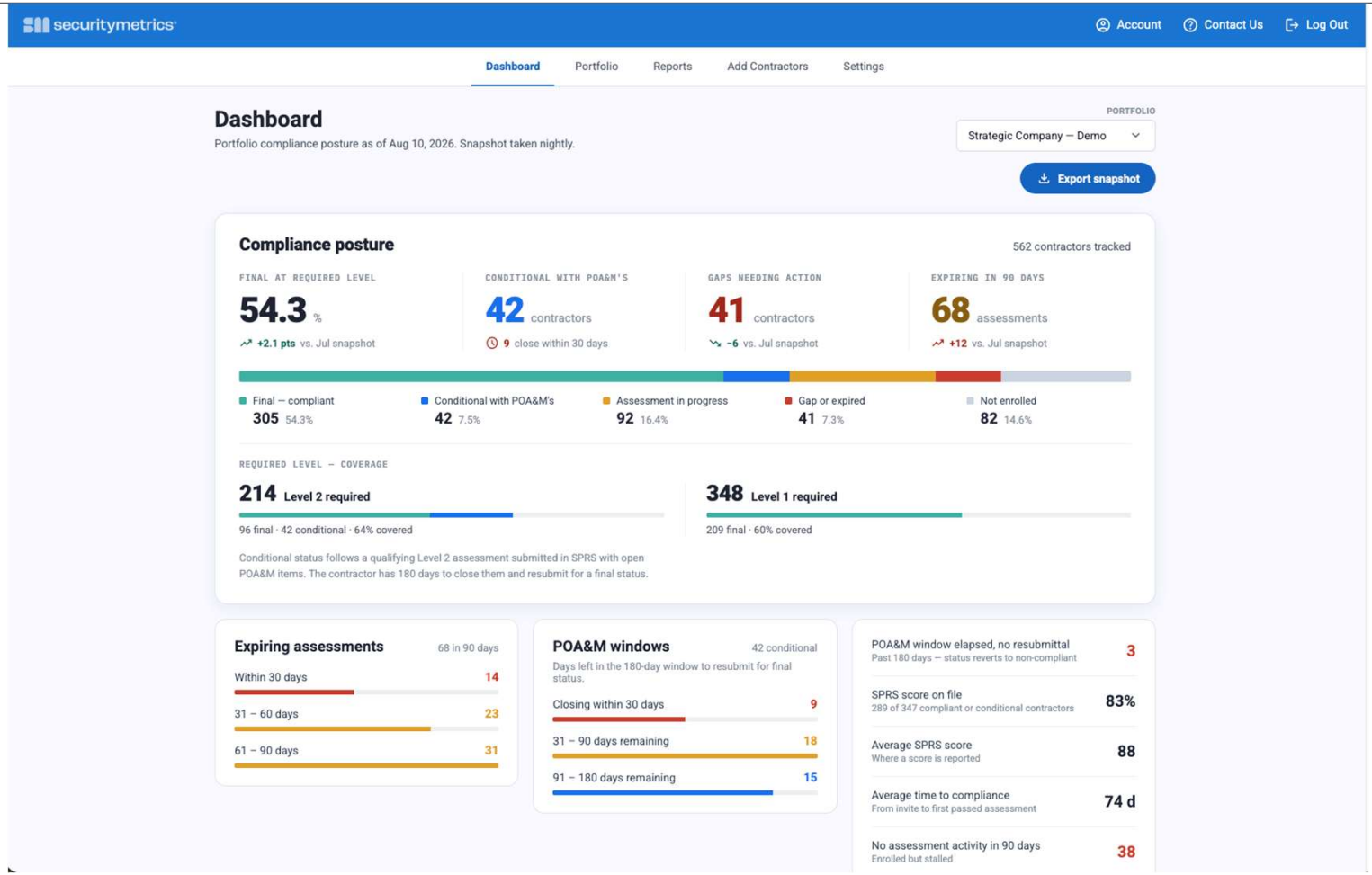


Working With Primes on CMMC Validation

- **L1 could have multiple primes or even a direct DoW connection**
- **Get definition of FCI being sent to you by a prime contractor**
- **Get clear direction from primes about what validation evidence they want**
  - L1 Self Assessment validation date
  - Affirming official details
  - SPRS screen shot(s)
- **Prime may want validation data added to a flow-down portal or provided via email**
- **Is there a compliance data aggregator you can enter once and report multiple times?**



Flow-Down Dashboard View



Summing Up

- Don’t orchestrate your own L1 compliance emergency
- Show contract readiness by finishing Self Assessment
- Proper scoping and evidence of compliance determines whether you pass a self assessment, its not just a checkmark
- Get going now, it feels better when you are done
- Help is available - portals, consultants, and good network design (segmentation, enclave, etc.) can help you get it done

securitymetrics®

Questions?

gglover@securitymetrics.com

Booth in the back

See me at Table Talks, today 2:45 PM – Free consulting today!