LET’S CUT THE BS

By: Andy Sauer

August 18, 2026

SENTINELBLUE

DISCLAIMERS

- These are my opinions.

CMMC TODAY

UNCERTAINTY IS THE NORM

- 8 years since DFARS 7012.
- ~18 months of stable, forward progress.
- Back to uncertainty.
- So what do we do with uncertainty?

THE FITNESS TEST

- Imagine I tell you that someday in the near future, we're going to test your physical fitness, but I don't tell you anything specific.
- Could be weightlifting, could be distance running, could be flexibility.
- What would you do?

Take action to get in shape.
Do you really need all the specifics?

CYBER FITNESS

- We know that the DoW cares about cybersecurity in the DIB.
- They may move the goalposts, they may not.
- But don’t let it tempt you into inaction.
- Get into shape.

WORDS TO LIVE BY

DEALING IN INFORMATION

- **CMMC and the surrounding ecosystem is esoteric**
  - Dozens of authoritative publications on different topics.
  - Different authorities in different agencies.
  - Many, many interpretations.
- **Generally well-meaning people say things that sound authoritative and that make sense.**
- **This gives rise to common "misinformation" – not out of bad intent.**
  - A bad game of telephone can leave you looking foolish at the end.

“Where is that written?”

- You, said frequently.

GETTING CLARITY (AND EQUIPPING YOURSELF)

- **It starts in 32 CFR 170.**
  - **The regulatory text controls**. Not the CAP. Not the guides.
- **Your first line of "defense" here is knowledge.**
  - You don't need to be a lawyer.
  - But you do need to be aware.
- **NIST References Matter**

"Are we describing a **risk**, or are we describing a **requirement**?"

- Ryan Bonner

RISKS AREN'T REQUIREMENTS

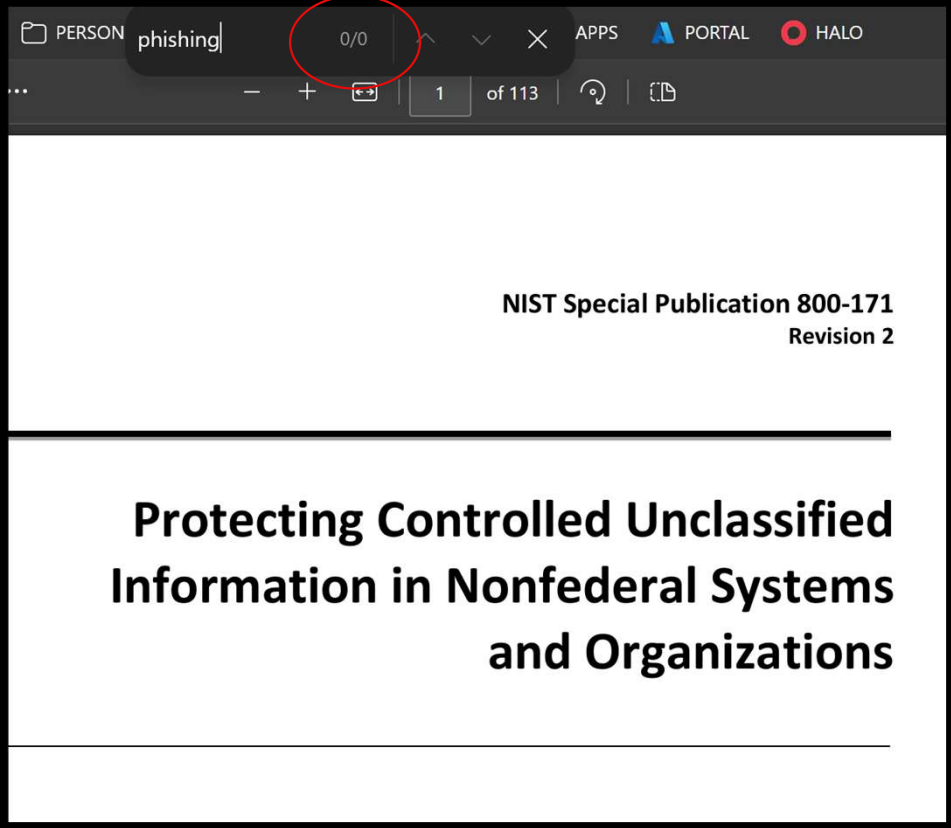
- **Many things we see circulated in the ecosystem make sense.**
  - But they aren't requirements.
- **"Where is that written?"**
  - It's a hard question – but you should be asking them of your advisors, consultants, C3PAOs. They should have good answers.

PHISHING FOR ANSWERS

- What remains the leading cause of compromise?

PHISHING FOR ANSWERS

- What remains the leading cause of compromise?
- Addressing phishing isn't in the requirement, but it sure is a risk.



PHISHING FOR ANSWERS

- If your security person tells you that you must address phishing specifically to be 800-171 compliant, you have a problem.
- If your security person tells you that you don't need to address phishing, because its not an 800-171 requirement, you have a problem.

CHALLENGING REQUIREMENTS

- Understanding risks vs. requirements matters.
- Being prepared to defend *risk decisions* as *risk decisions* pays dividends in assessments.
- Don't let risks be treated as requirements.
- Understanding the requirements is your best tool.

WHAT REGULATIONS SAY

EXAMPLE: ESPS & CSPS PER 32 CFR 170

External Service Provider (ESP) means external people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (*e.g.*, log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. (CMMC-custom term)

Cloud Service Provider (CSP) means an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This definition is based on the definition for cloud computing in NIST SP 800-145 Sept2011. (CMMC-custom term)

WHEN IS AN ESP A CSP?

From 2011, by the way.

- NIST 800-145 "Cloud Computing":
  - "a model for enabling ubiquitous, convenient, **on-demand network access** to a s**hared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be **rapidly provisioned** and released **with minimal management** effort or service provider interaction."

WHEN IS AN ESP A CSP?

- **NIST 500-322 "Evaluation of Cloud Computing":**
  - Five essential characteristics
    - On-demand self-service
    - Broad network access
    - Resource pooling
    - Rapid elasticity
    - Measured service

WHEN IS AN ESP A CSP?

- 500-322 says:

Essential Characteristics: The five characteristics that must be available in a computing capability to be qualified as a "cloud service." They are listed here for clarity, but are discussed in greater detail in Section 3.

- on-demand self-service (see section 3.1)
- broad network access (see section 3.2)
- resource pooling (see section 3.3)
- rapid elasticity (see section 3.4)
- measured service (see section 3.5)

To understand the essential characteristics, it is important to understand the meaning of the term "essential." In the context of SP 800-145 and this document, "essential" means each cloud service provider (CSP) must have the ability to provide each essential characteristic to the cloud service customer (CSC) for a given service. The CSC may or may not elect to implement or use each essential characteristic in a specific instance. In addition, the CSC must make a subjective judgement to determine

>> IF IT WERE ONLY SO SIMPLE.

PURPOSE OF 500-322

- Not exactly written for determining risk/scoping.

Requirement 4 of the Roadmap is for "Clearly and consistently categorized cloud services." This requirement is important to ensure that customers understand the characteristics of different types of cloud services and are able to objectively evaluate, compare, and select cloud services suitable to meet their business objectives.

In the absence of clarification, organizations are at risk of adopting "services" that do not provide characteristics of cloud computing. For example, some vendors reportedly decide to label their computing offerings as "cloud services," even if the offerings do not support the essential characteristics of a cloud service in the NIST definition.

Furthermore, the frequent and common usage of the informal "aaS" (as a Service) suffix in marketing, as in "EaaS" (Enterprise as a Service), "DaaS"(Desktop as a Service or Data as a Service), "STaaS" (Storage as a Service, and even "XaaS" (Everything as a Service) is confusing, and (unintentionally) obfuscating the architecturally well-founded distinction of Software as a Service (SaaS), Platform as a Service, (PaaS), and Infrastructure as a Service (IaaS). These "cloud service types" are generally coined by appending the suffix "aaS" after a type of computing capability or marketing term. This makes it difficult to determine whether something is a cloud service and has unintended consequence for organizations trying to satisfy their cloud-first objectives.

500-322 FINAL

As this document is meant to provide guidance in understanding the categorization, evaluation, comparison, and selection of cloud services, it does not provide a prescriptive set of guidelines for the selection process. Instead, it uses the principles set forth in the NIST cloud computing definition as a framework for understanding a customer's requirements in a cloud computing context and the capabilities offered by cloud service providers (CSP)s to enable easier decision making. The NIST cloud computing definition allows for flexibility in its interpretation and in many cases, the final decision relies on a mixture of objective and subjective perspectives.

SO, WHERE'S THE CLARITY?

- It's a matter of risk profile.
- A CSP and an MSP have different risks they pose to the ecosystem.
- But it's going to be subjective. Because the requirements aren't crystal clear.
- There are dozens of questions/challenges like this.

REGULATORY GAPS

- When exactly has a significant change occurred?
- How much effort does a certified ESP get to have reduced?
- How many controls can I inherit?
- Is the *potential* to touch CUI enough to force FedRAMP requirements?

If you’re looking for binary answers, we don’t have them.

WHAT CMMC REQUIRES, BROADLY

- **CMMC mostly requires capabilities and functions to be in place.**
  - "Have an Incident Response plan"
  - "Ensure only authorized users, processes and devices have access."
  - "Train your people to the risks they face."
- **It's rarely specified in hard numbers.**
  - "A time within which to identify flaws is specified" (they mean by **you**).
  - 800-171r3 and ODPs may change this somewhat

WHAT PEOPLE SAY

EVEN THE EXPERTS DISAGREE

- There is a whole ecosystem of CMMC experts who spend hundreds of hours debating amongst ourselves about interpretations.
- This means *you must be informed*.
  - You must be prepared to make informed, risk-based decisions about unclear requirements.

“YOU CAN’T OUTSOURCE RESPONSIBILITY”

- **OSC holds ultimate accountability and responsibility.**
  - The liability stays with the OSC; OSC signs the contract.
- **“You can’t outsource this control.”**
  - I’m skeptical. There’s no regulatory statement listing which controls can be fulfilled by an ESP vs. not.
    - The AB has listed some examples in town halls – is that binding?
  - Keep it feasible.
- **Use a reasonable approach to all things**
  - **The right intent goes a long way, even if you’re wrong.**

RECOMMENDATIONS

- **Collaborate, Don't Agitate.**
  - Share the information. Show the SSP. Build the confidence.
- **Risk decisions should be feasible. Don't be ridiculous.**
- **Establish consensus in or before Phase 1.**
  - C3PAOs get to be subjective; you can be subjective in choosing your C3PAO.
- **Equip yourself.**

WORDS TO LIVE BY

- “Where is that written?”
- “Are we describing a risk, or describing a requirement?”

LET'S NOT LOSE THE FOREST

- This is about addressing the real cybersecurity risks you face.
- There are real, every day threats seeking to damage your organization.
- Don't let the trees of regulatory confusion and uncertainty blind you to the forest that is protecting your organization.

THANK YOU