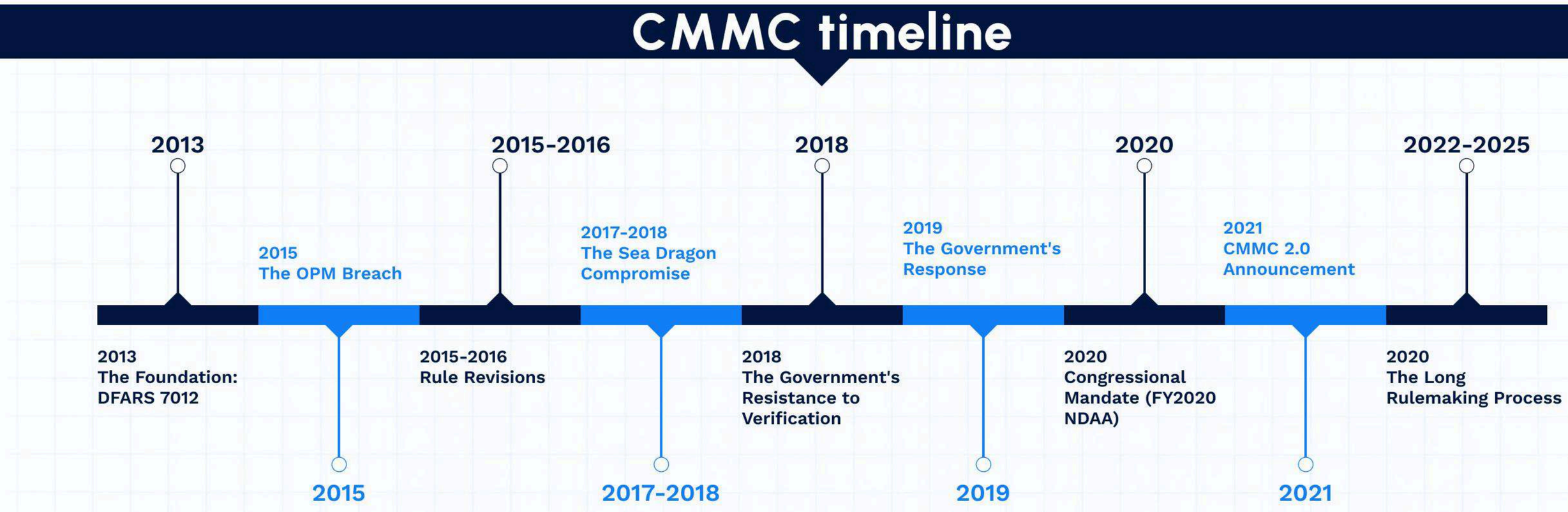
eSHARE

The History of CMMC 2.0: How We Got Here

Mike Towers
Chief Strategy & Trust Officer



2013

The Foundation: DFARS 7012

The story of CMMC begins over a decade before most people realize. In 2013, the Department of Defense created DFARS clause 252.204-7012 for the first time. Before this, defense contractors had no explicit cybersecurity requirements in their contracts whatsoever to protect Controlled Unclassified Information (CUI) - sensitive defense data like technical specifications, acquisition details, and export-controlled information.

The original 2013 clause pulled 59 security controls from NIST SP 800-53 (since NIST SP 800-171 didn't exist yet). However, there was a critical flaw: no verification mechanism existed. Contractors simply accepted the clause and were trusted to comply, with no audits or proof required.

2015

The OPM Breach

In 2015, the Office of Personnel Management experienced one of the largest compromises of federal information systems in history. The Chinese Ministry of State Security combined data from the OPM breach with information from hotel chains and health insurance companies to identify American intelligence operatives in mainland China.

This breach exposed a major gap: the 2013 requirements didn't adequately cover cloud systems and sensitive unclassified information like clearance data.

2015-2016

Rule Revisions

After the OPM breach, the DoD issued an interim final rule in August 2015 - a rare regulatory action that bypasses normal public comment periods due to national security urgency. This revision:

- Added cloud security requirements (FedRAMP Moderate equivalency)
- Replaced the 59 controls from NIST 800-53 with the requirements from newly published NIST SP 800-171 (110 requirements)

Interestingly, even though NIST 800-171 listed 110 requirements compared to the original 59 controls, the actual implementation effort was often smaller because the requirements were more precisely scoped with fewer assessment objectives to prove compliance.

Industry Pushback

Despite the emergency nature of the breach, industry immediately requested more time to implement the requirements. After a public meeting in December 2015, the DoD granted an extension. The October 2016 update established the December 31, 2017 deadline that became infamous in the contractor community.

Remarkably, even after two major national security incidents, there was still no third-party verification mechanism.

2017-2018

The Sea Dragon Compromise

Just a couple years after the government's adamant opposition to verification, another massive breach occurred. Chinese cyber operations compromised unclassified contractor systems, stealing data from major programs including:

- F-35 and F-22 fighter programs
- Sea Dragon: A submarine-launched hypersonic anti-ship missile program

The Sea Dragon compromise was particularly damaging because China's submarine fleet is the largest in the world, and these weapons are critical to defending Taiwan from potential Chinese takeover.

2018

The Government's Resistance to Verification

At a 2018 industry day presentation, someone in the audience asked why there was no requirement to prove compliance. The response was telling:

- Gus Gasani (NIST 800-171 author): "The department does not want to have a cottage industry of non-value-added [assessments]. We had experience with third-party assessments before, and it has not worked out well."
- Devin Casey (NARA CUI rules author): Businesses already have the cybersecurity knowledge and ability to protect information "because they've already been doing so for years."

The DoD and NARA explicitly stated they did not want third-party assessments unless "absolutely necessary."

2019

The Government's Response

Major General Murphy, appointed by Secretary of Defense Mattis to lead the Protecting Critical Technology Task Force, gave a blistering interview in 2019:

"I would rather have this be a conversation than an explicit direction. But as unfortunately we've seen over the years, if there's no repercussions to not having security, there's no incentive to have it."

His message was clear: contractors who won't protect critical technology should not have DoD contracts.

The Inspector General Report

An IG investigation revealed the extent of the problem:

- Contractors were not implementing required security controls
- Contracting officers never asked for proof of compliance
- There were no consequences for non-compliance
- The entire system operated on trust that was clearly misplaced

2020

Congressional Mandate (FY2020 NDAA)

The Senate Armed Services Committee had seen enough. In the FY2020 National Defense Authorization Act, Section 1648 explicitly directed the DoD to:

"Create a framework that is going to hold contractors accountable and make them prove that they are implementing the requirements that are in their contracts."

The accompanying report stated: "We believe that the prime contractors need to be held responsible and accountable for securing Department of Defense technology and sensitive information."

This is why CMMC exists; Congress mandated it. The program is not the DoD's invention but rather Congress's response to repeated catastrophic failures.

CMMC 1.0 (2020)

In 2020, the DoD released CMMC 1.0 as another interim final rule - the second emergency rulemaking in five years addressing the same fundamental problem. The rule came out at the end of the first Trump administration.

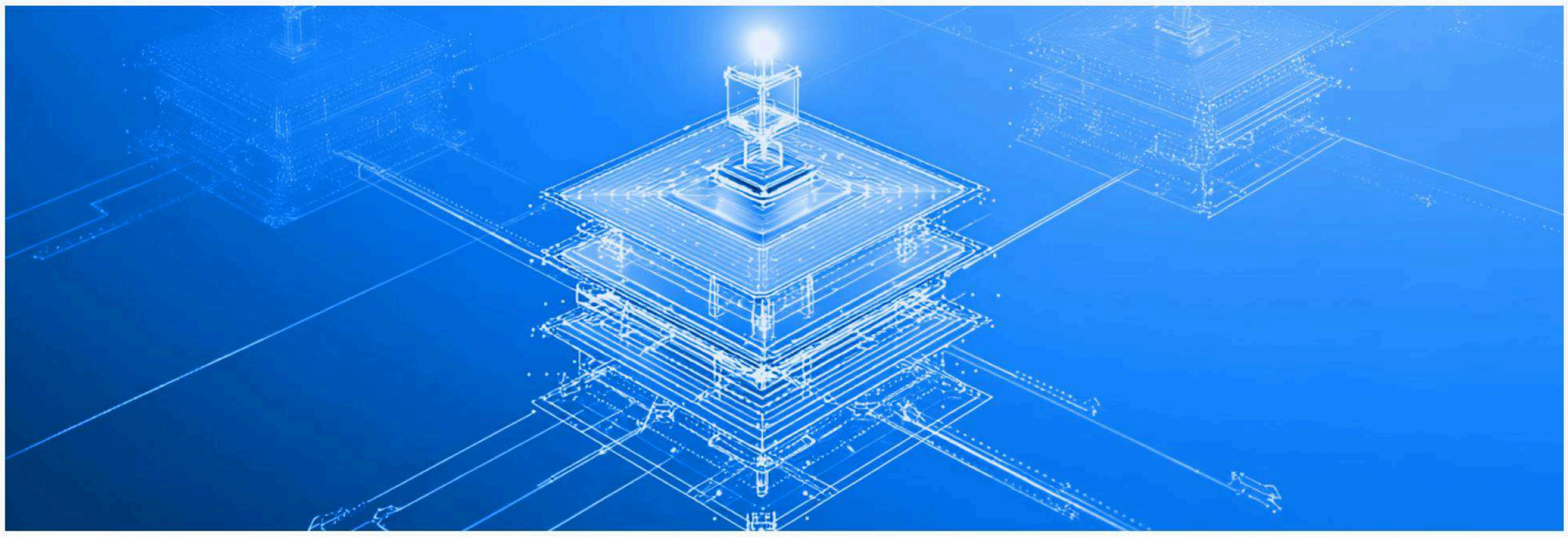
When the Biden administration took over in 2021, the standard regulatory review process began, and CMMC disappeared from public view for nine months. Many assumed it was dead.

2021

CMMC 2.0 Announcement

At the end of 2021, the DoD announced CMMC 2.0 and committed to additional rulemaking, including a new rule in Title 32 of the Code of Federal Regulations. When people heard "up to two years of rulemaking," many concluded CMMC was delayed indefinitely.

However, the commitment to modify 32 CFR (the assessment procedures) and 48 CFR (the contract language) - a significant bureaucratic undertaking - signaled that the new administration was doubling down on the program, not abandoning it.



2022-2025

The Long Rulemaking Process

The DoD expected to issue another interim final rule with CMMC going into contracts in spring 2023. However, the Office of Management and Budget (OMB) denied interim final status, requiring the standard rulemaking process instead.

The Rulemaking Timeline:

December 2023

Proposed 32 CFR rule published (assessment procedures)

October 2024

Final 32 CFR rule published

December 2024

32 CFR rule became effective (market rollout began)

September 2025

Final 48 CFR rule published (updated DFARS clause language)

Nov 10, 2025

Phase 1 begins; CMMC requirements start appearing appears in new DoD solicitations and contracts

Why CMMC Won't Go Away

Throughout this journey, people repeatedly predicted CMMC's demise: when administrations changed, when leadership changed, when rulemaking was announced, when delays occurred.

But the program has consistently survived because:

1. **Congressional mandate:** The same lawmakers who wrote Section 1648 largely remain on the Armed Services Committee
2. **Bipartisan support:** The program has survived transitions between politically opposed administrations
3. **Ongoing threat:** The national security problems that prompted CMMC haven't been solved, they've worsened
4. **No alternative:** After 12+ years of contractors not implementing required controls despite having them in contracts, verification is the only viable path forward

Key Takeaway

CMMC is not creating new requirements. The cybersecurity requirements have existed since 2013 (and in smaller form, even earlier). CMMC is the verification program that proves contractors are actually implementing what they've been contractually obligated to do for over a decade.

As one frequently quoted observation notes: "CMMC is different from the requirements that it's verifying. It's making sure you did the requirements - it's not making you do anything new."

After more than 12 years, multiple administrations, several Secretaries of Defense, countless breaches, two interim final rules, Congressional mandate, and extensive rulemaking, CMMC Phase 1 begins November 10, 2025. This marks not an ending, but the beginning of the "new normal" for DoD contracting.

Mike Towers

Chief Strategy & Trust Officer

The History of CMMC 2.0: How We Got Here

---

eSHARE

About eSHARE

Get in touch to weave your Trusted Collaboration Fabric. eSHARE secures every share while teams move faster with intelligent, Zero-Trust guardrails.

LinkedIn

Contact Us

www.eshare.com