United Rotorcraft

Supplier CMMC Readiness

March 27, 2025

Event Agenda

- **10:00 AM Review Agenda & Introductions**
- United Rotorcraft Opening
- United Rotorcraft Presentation
- Manufacturer’s Edge Project Focus
- **Break**
- Synagex Presentation
- Core Business Solutions Presentation
- Sustainment Demo
- Pricing & Final Questions
- ME Sign Up
- **12:00 PM Survey & Event Closeout**

Introductions

United Rotorcraft®

- Carlos Hernandez
  Contracts Admin & CX Services Mgr.
- Dan Kaminski
  Sr Manager of Supply Chain
- Justin Johnson
  Sr Dir Safety & Quality
- Michael Knight
  QA Supervisor & Exports Empowered Official

MANUFACTURER'S EDGE

- Rob Newbold
  Vice President, Client Success Team
- Jennifer Hagan-Dier
  Vice President & Chief Operating Office
- Ryan Burns
  Supply Chain Specialist

Presentation Agenda

- Opening
- Fundamental Questions
- Background: CMMC 2.0
- Project Overview
- Questions?
- References

Opening

Why are we doing this?

- CMMC Program is now law
- This is a flow-down requirement
- Supply chain alignment with regulations
- Avoid business interruption
- Avoid legal fees

What are we going to do?

- Provide background on CMMC
- Outline the program approach

How are we going to do it?

- Assess, Implement, Manage

When will this effort begin?

- Today. The aim is to onboard you starting by April

What we need from you

- Sign-Up for a no-cost appointment with ME by April 3rd, 2025
- Have available your DFARS compliance scorecard uploaded via the Sustainment platform by April 15, 2025
- Your cooperation

Position suppliers for success by achieving CMMC readiness for business continuity

Fundamental Questions | CUI & DFARS

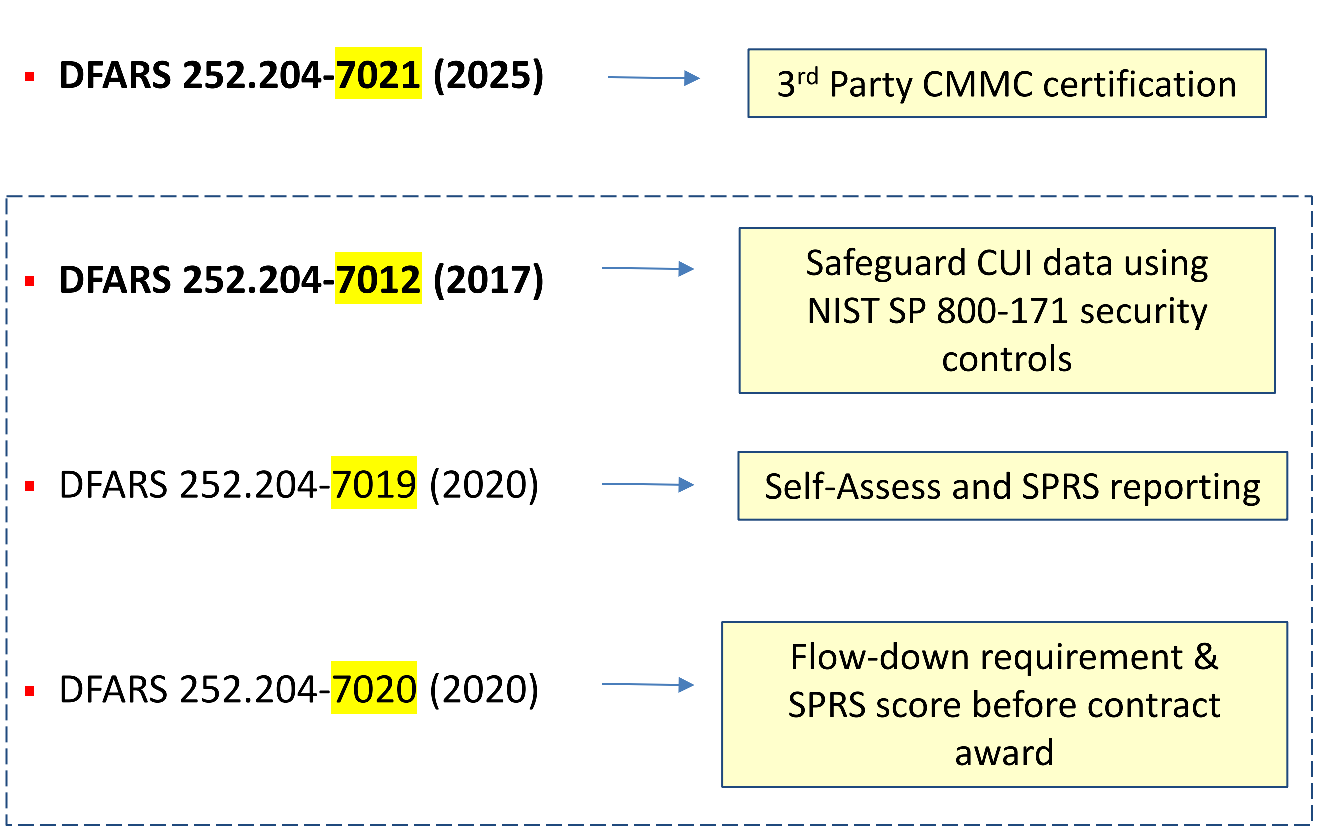
What is CMMC?

- CMMC stands for Cybersecurity Maturity Model Certification.
- A DoD certificate program designed to enhance the cybersecurity practices
- It is broken as a three-tiered model
  - Level 1: Foundational
  - Level 2: Advanced
  - Level 3: Expert

What is CMMC's purpose?

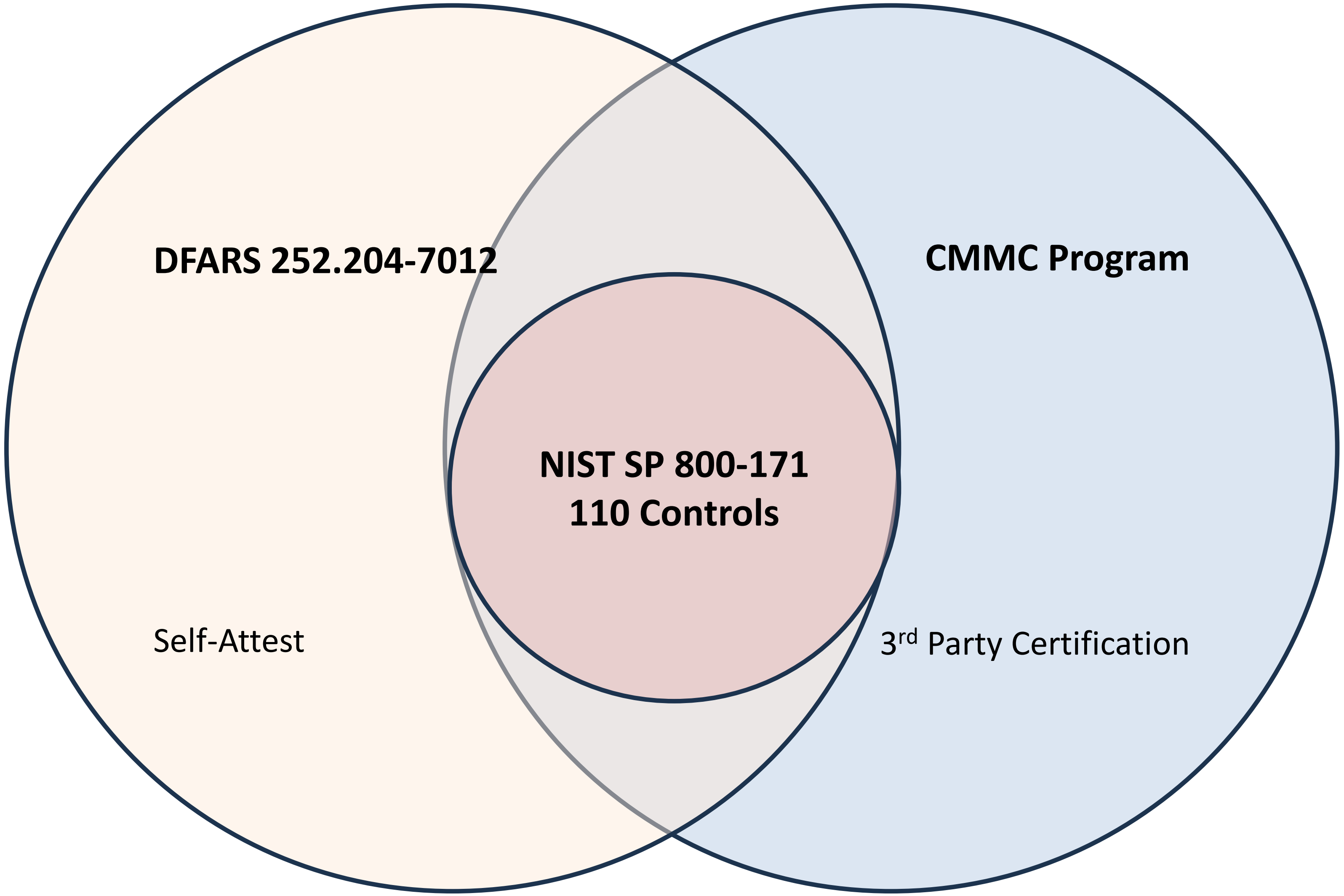
- Protect sensitive information
- Controlled Unclassified Information (CUI)

Which DFARS shall I pay attention to when reviewing my contract?



- **DFARS 252.204-7021 (2025)** → 3rd Party CMMC certification
- **DFARS 252.204-7012 (2017)** → Safeguard CUI data using NIST SP 800-171 security controls
- DFARS 252.204-7019 (2020) → Self-Assess and SPRS reporting
- DFARS 252.204-7020 (2020) → Flow-down requirement & SPRS score before contract award

Fundamental Questions | CUI & DFARS



DFARS 252.204-7012

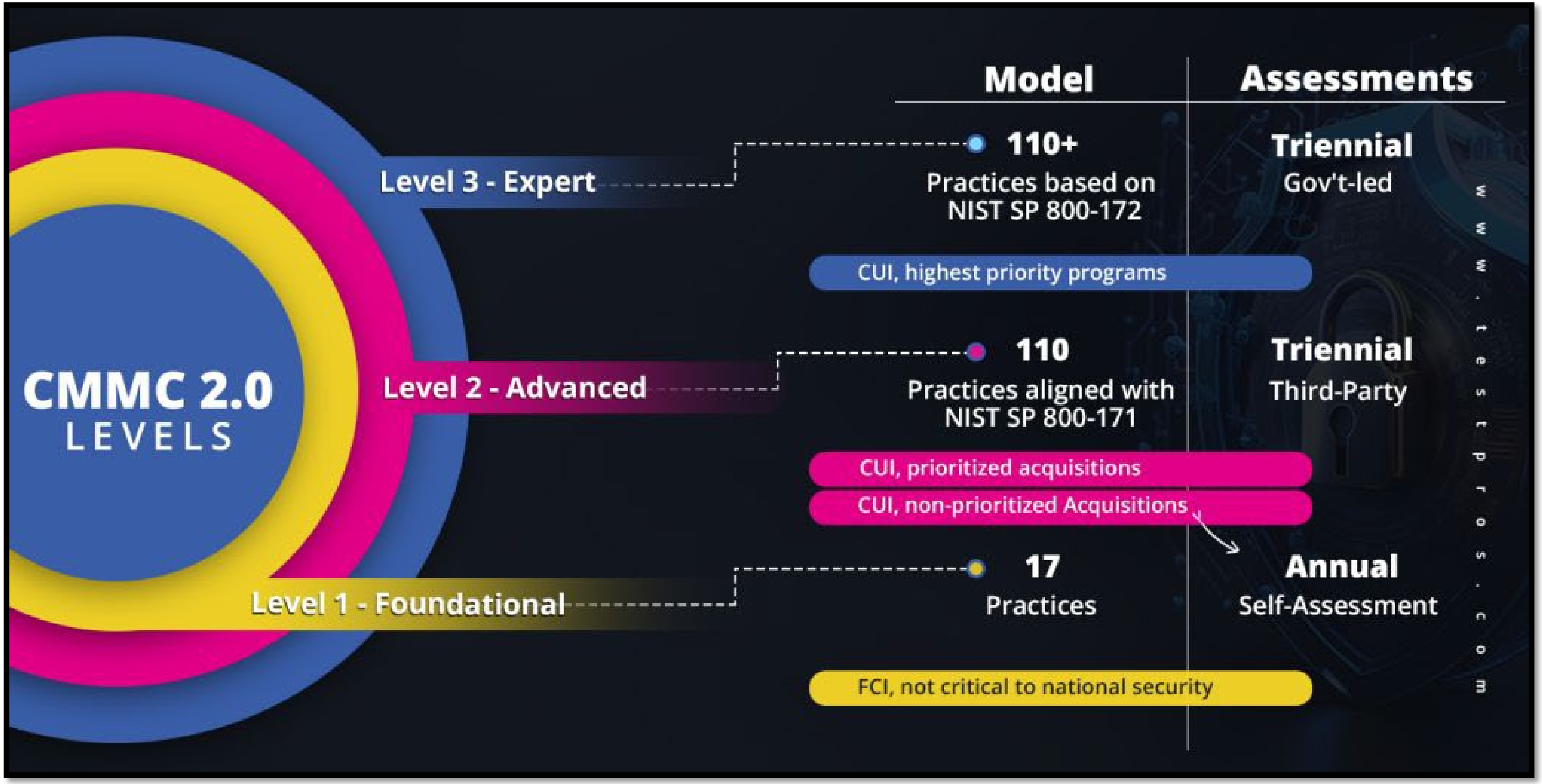
Self-Attest

CMMC Program

3rd Party Certification

NIST SP 800-171
110 Controls

Background: CMMC 2.0

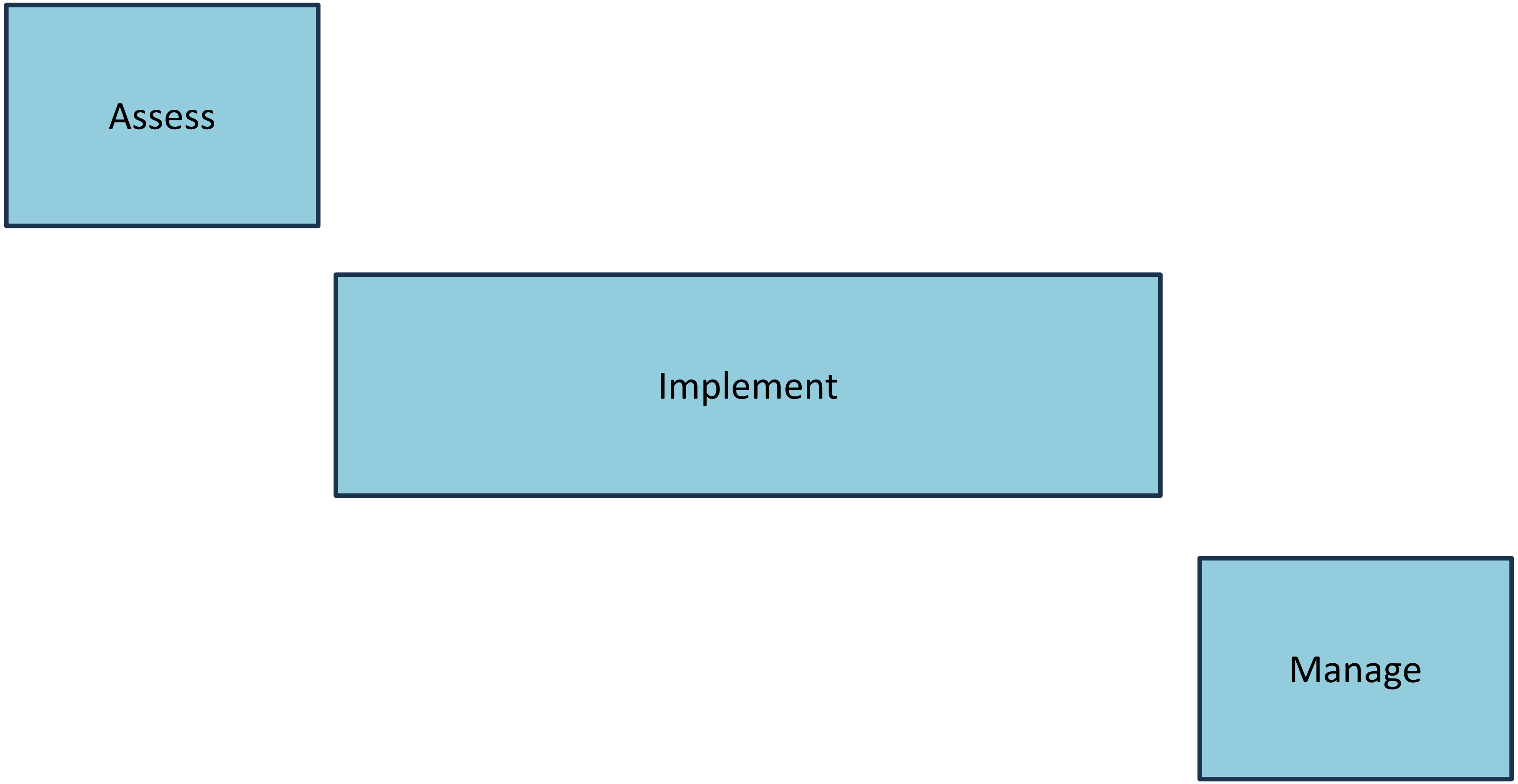


CMMC 2.0 LEVELS

	Model	Assessments
Level 3 - Expert	110+ Practices based on NIST SP 800-172 CUI, highest priority programs	Triennial Gov't-led
Level 2 - Advanced	110 Practices aligned with NIST SP 800-171 CUI, prioritized acquisitions CUI, non-prioritized Acquisitions	Triennial Third-Party
Level 1 - Foundational	17 Practices FCI, not critical to national security	Annual Self-Assessment

Project Overview - Approach

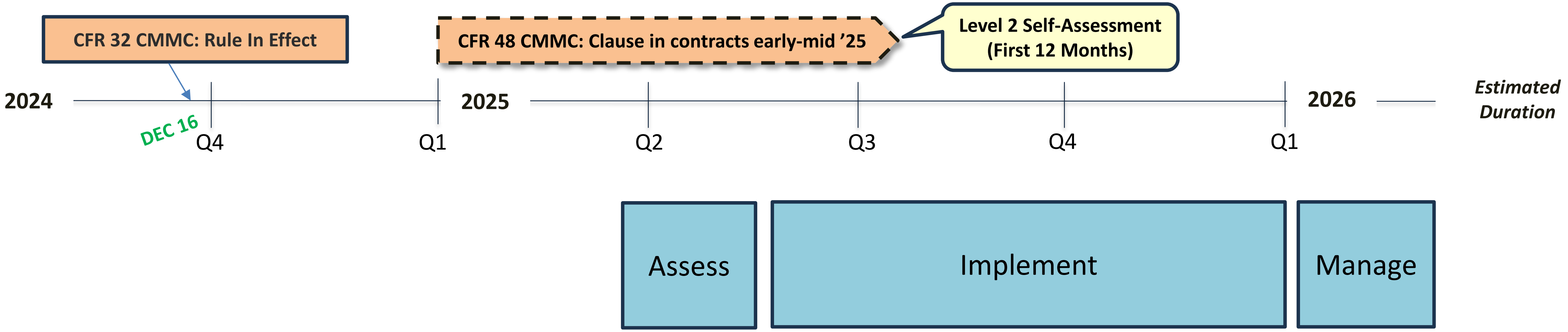
Key Objective


Assess

Implement

Manage

Project Overview – Timeline



CFR 32 CMMC: Rule In Effect

CFR 48 CMMC: Clause in contracts early-mid ’25

Level 2 Self-Assessment
(First 12 Months)

2024

DEC 16

Q4

Q1

2025

Q2

Q3

Q4

Q1

2026

Estimated Duration

Assess

Implement

Manage

Questions?

ME - Sign Up QR Code and Link

MANUFACTURER'S EDGE

https://manufacturersedge.com/cmmc-supplier-readiness-program/

UR - Survey QR Code and Link

United Rotorcraft®

https://airmethods.co1.qualtrics.com/jfe/form/SV_8x0bpV18TjJhOgC

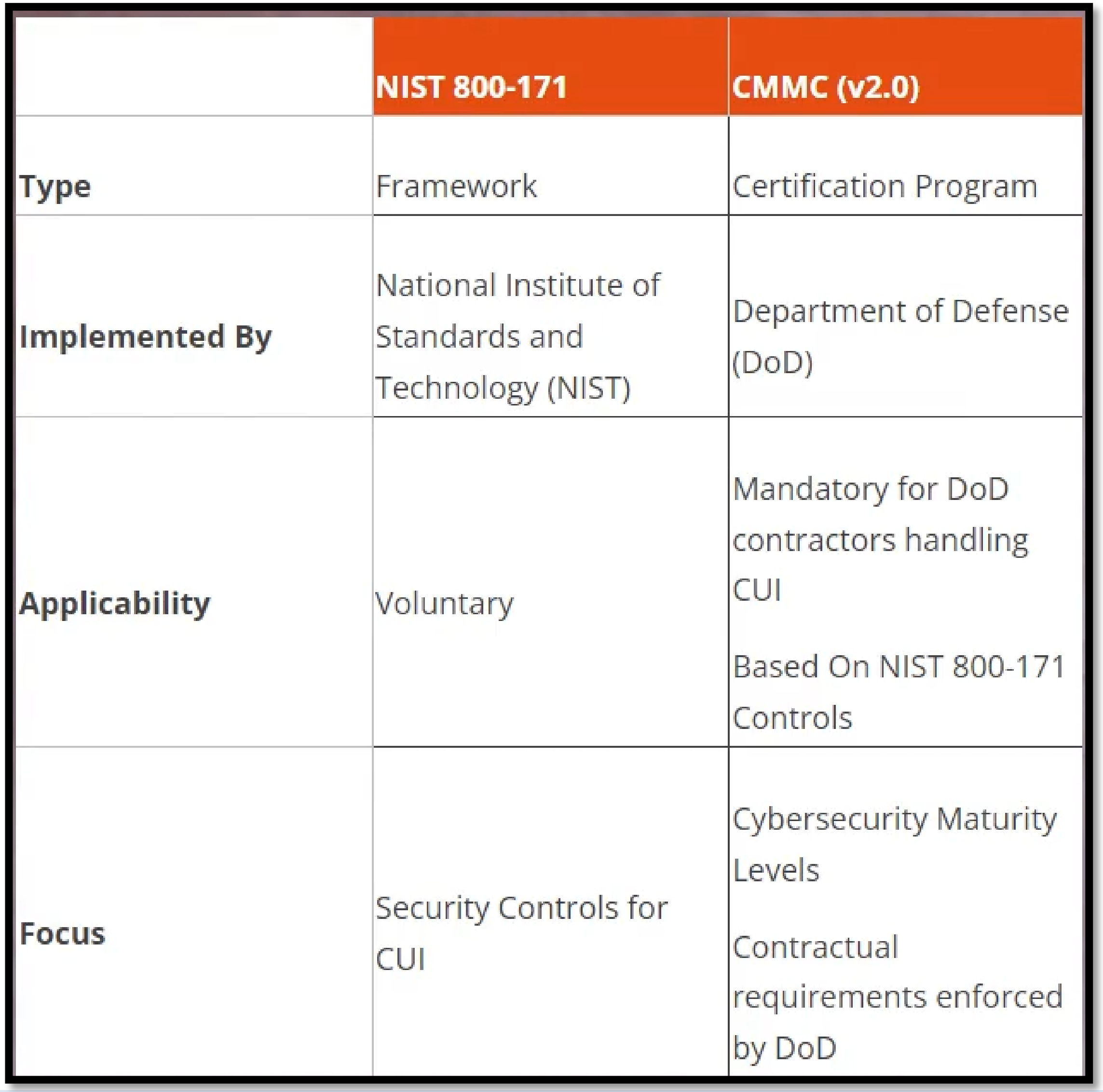
References

- 9/11 Commission Report: https://www.govinfo.gov/app/details/GPO-911REPORT/summary
- 14 NIST Families: https://www.cnc-west.com/j-j-machining-nist-800-171-compliance-is-here-this-aerospace-manufacturer-is-on-the-front-lines-of-cyber-security/
- Understanding the 14 NIST control families: https://www.kelsercorp.com/blog/14-nist-control-families
- CFR 32 and CFR 48: https://www.govconwire.com/2024/08/govcon-expert-payam-pourkhomami-analyzes-differences-between-cfr-32-and-cfr-48/#:~:text=While%20CFR%2032%20provides%20the,for%20short)%20comes%20into%20play.
- CFR 32 and 48 Timeline: https://redspin.com/resource-center/infographics/
- NIST 800-171 vs. 800-53: https://www.encompassconsultants.com/article-posts/nist-800-171-vs-800-53-why-theyre-different-comparison
- CIO About CMMC: https://dodcio.defense.gov/CMMC/about/
- CMMC 2.0 Levels: https://testpros.com/articles/cmmc-preparedness-through-nist-sp-800-171-revision-3/
- CFR 32 and CFR 48 Timeline and Projections: https://www.linkedin.com/posts/redspin-inc_its-been-a-long-road-for-cmmc-with-milestones-activity-7274448457401012224-dIqy
- NIST SP 800-171 Controls chart: https://www.getpeerless.com/complete-guide-nist-800-171
- NIST Definition of SSP: https://www.pivotpointsecurity.com/ssp-for-cmmc-compliance/

CMMC Readiness

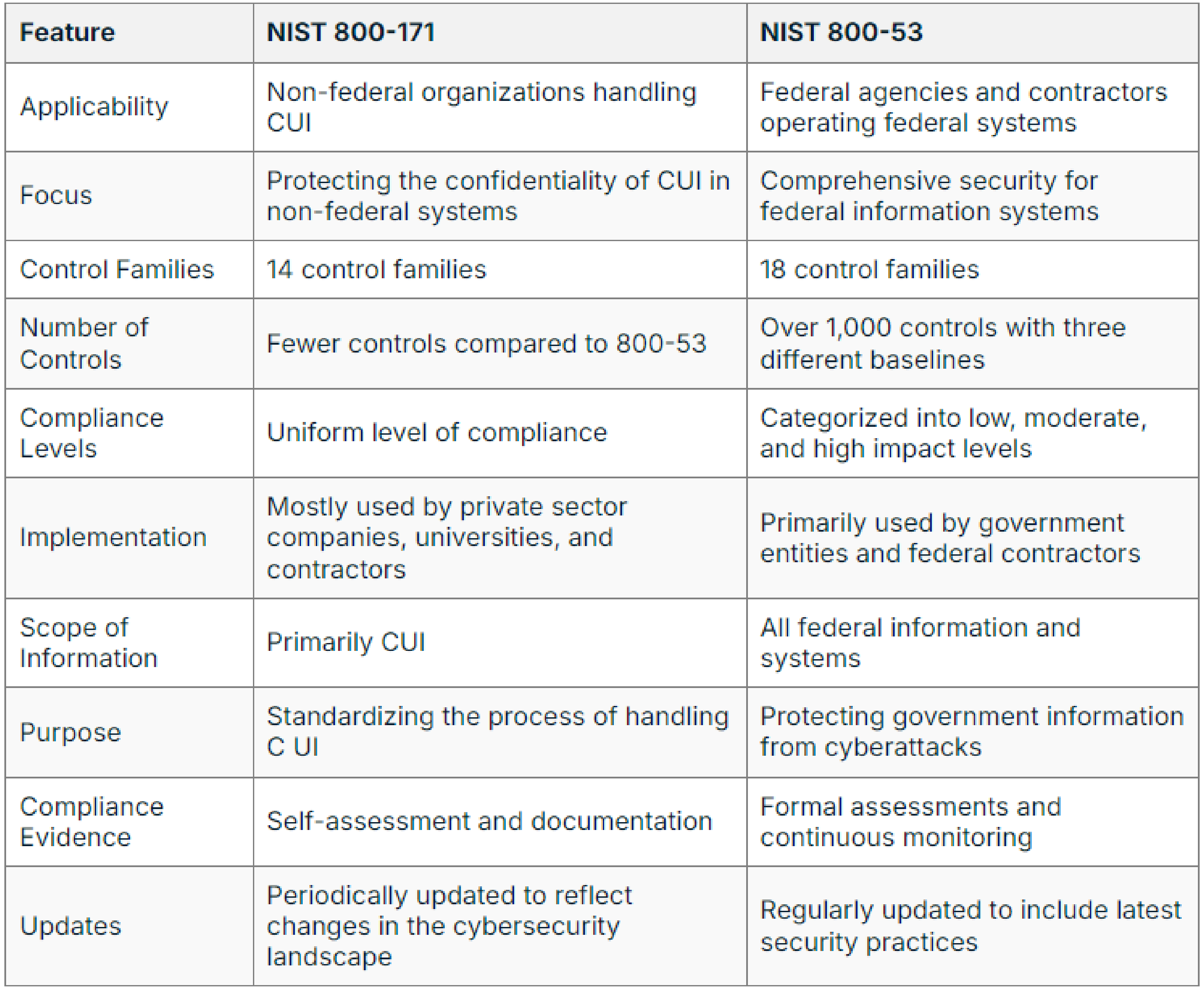
APPENDICES

NIST SP 800-171 vs CMMC 2.0



	NIST 800-171	CMMC (v2.0)
Type	Framework	Certification Program
Implemented By	National Institute of Standards and Technology (NIST)	Department of Defense (DoD)
Applicability	Voluntary	Mandatory for DoD contractors handling CUI Based On NIST 800-171 Controls
Focus	Security Controls for CUI	Cybersecurity Maturity Levels Contractual requirements enforced by DoD

NIST SP 800-171 vs NIST 800-53

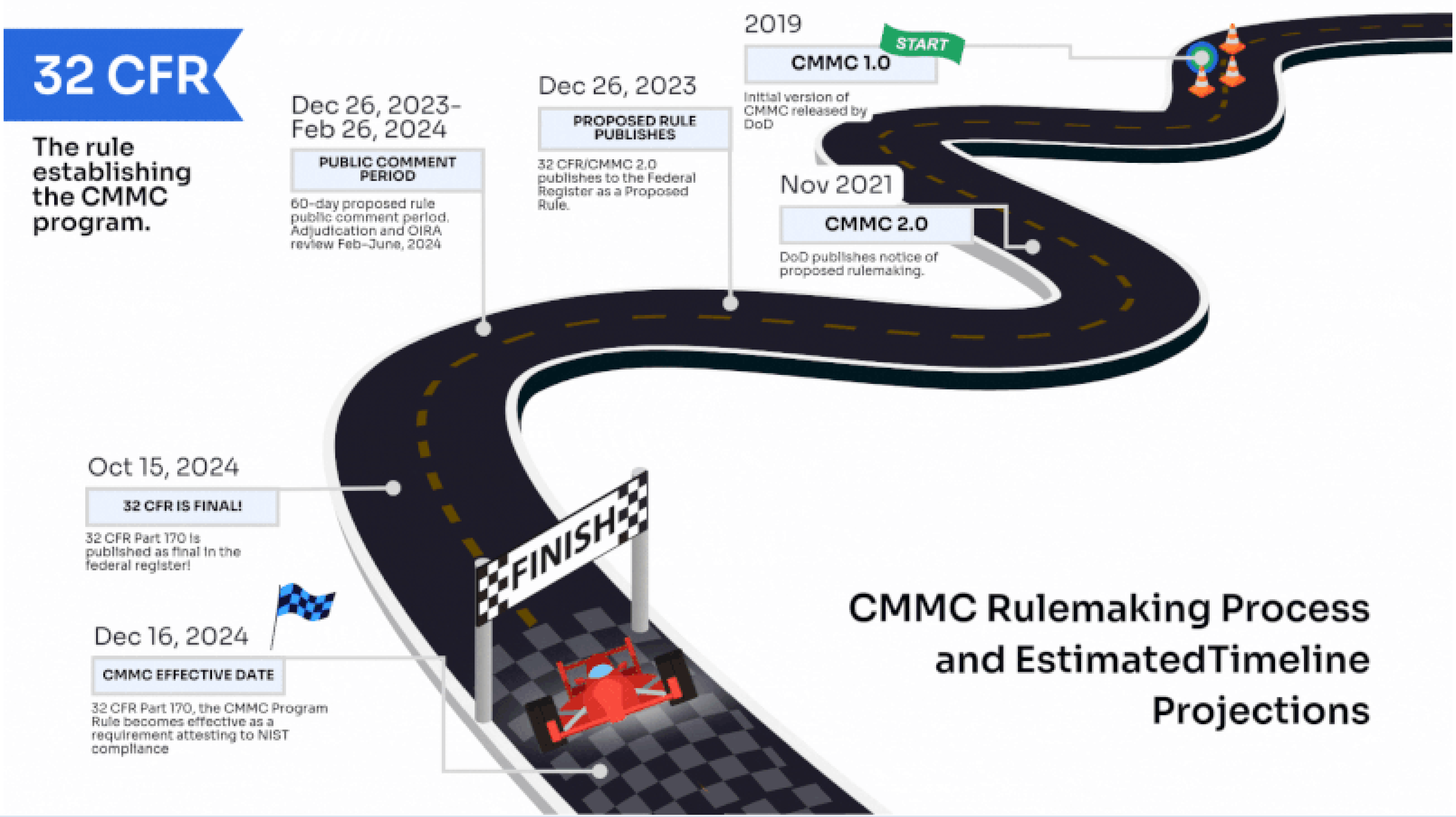


Feature	NIST 800-171	NIST 800-53
Applicability	Non-federal organizations handling CUI	Federal agencies and contractors operating federal systems
Focus	Protecting the confidentiality of CUI in non-federal systems	Comprehensive security for federal information systems
Control Families	14 control families	18 control families
Number of Controls	Fewer controls compared to 800-53	Over 1,000 controls with three different baselines
Compliance Levels	Uniform level of compliance	Categorized into low, moderate, and high impact levels
Implementation	Mostly used by private sector companies, universities, and contractors	Primarily used by government entities and federal contractors
Scope of Information	Primarily CUI	All federal information and systems
Purpose	Standardizing the process of handling C UI	Protecting government information from cyberattacks
Compliance Evidence	Self-assessment and documentation	Formal assessments and continuous monitoring
Updates	Periodically updated to reflect changes in the cybersecurity landscape	Regularly updated to include latest security practices

Code of Federal Regulations (CFR)

CFR 32: Blueprint for CMMC Implementation	CFR 48: Implementing CMMC in Federal Acquisitions
The foundation for CMMC, CFR 32 provides the comprehensive framework for the CMMC program. It is the cornerstone outlining CMMC as a three-tiered model: Level 1, 2 and 3	Facilitates the inclusion of the DFARS 252.204-7021 clause in defense contracts, making CMMC requirements enforceable contractual obligations. All federal contract clauses and provisions are codified in Title 48 of the CFR.

CFR 32 & 48 Timeline and Projections



32 CFR

The rule establishing the CMMC program.

2019

CMMC 1.0

Initial version of CMMC released by DoD

Nov 2021

CMMC 2.0

DoD publishes notice of proposed rulemaking.

Dec 26, 2023

PROPOSED RULE PUBLISHES

32 CFR/CMMC 2.0 publishes to the Federal Register as a Proposed Rule.

Dec 26, 2023-Feb 26, 2024

PUBLIC COMMENT PERIOD

60-day proposed rule public comment period. Adjudication and OIRA review Feb-June, 2024

Oct 15, 2024

32 CFR IS FINAL!

32 CFR Part 170 is published as final in the federal register!

Dec 16, 2024

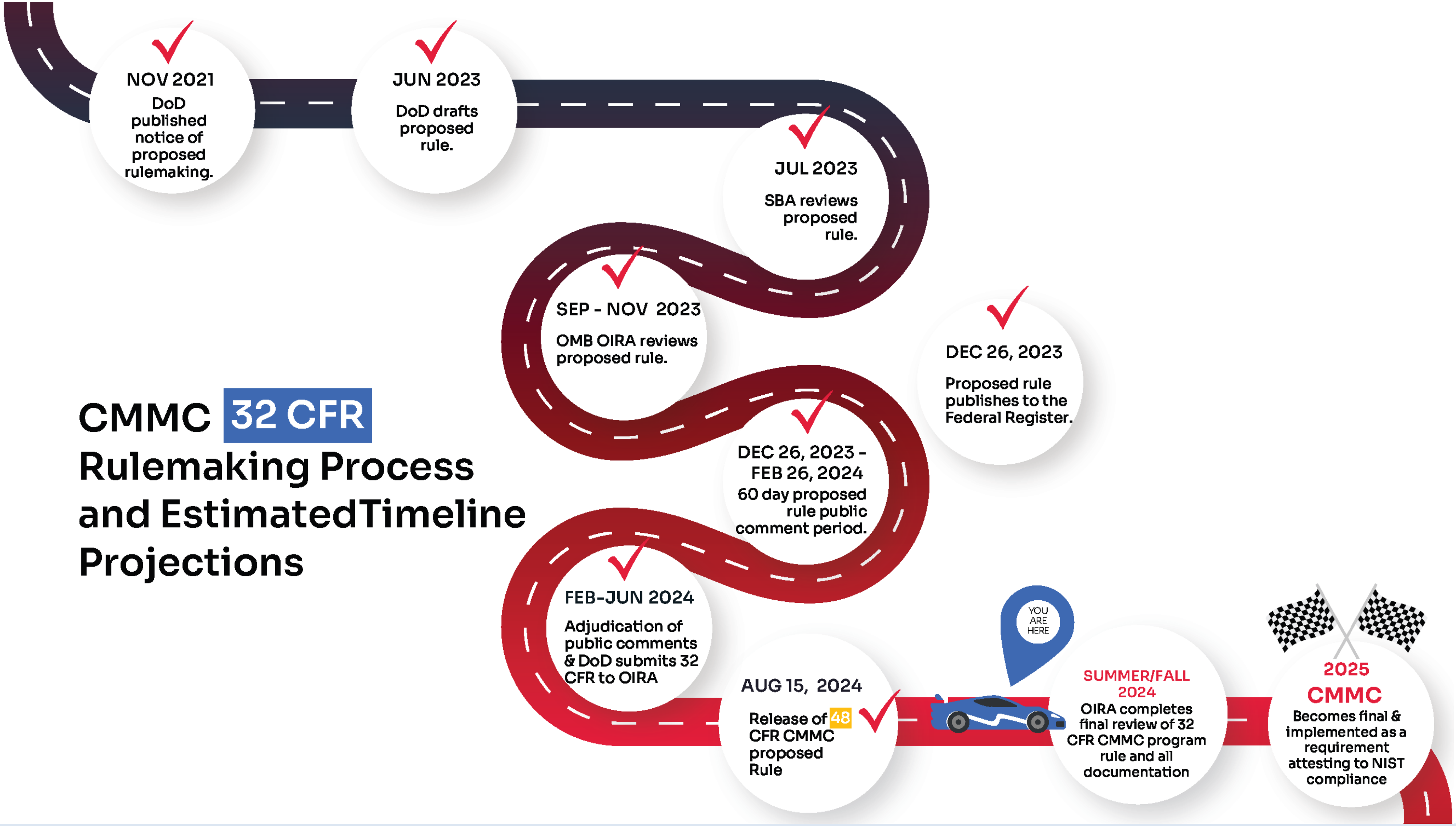
CMMC EFFECTIVE DATE

32 CFR Part 170, the CMMC Program Rule becomes effective as a requirement attesting to NIST compliance

CMMC Rulemaking Process and EstimatedTimeline Projections

CFR 32 Timeline

CMMC 32 CFR Rulemaking Process and EstimatedTimeline Projections



✓ NOV 2021
DoD published notice of proposed rulemaking.

✓ JUN 2023
DoD drafts proposed rule.

✓ JUL 2023
SBA reviews proposed rule.

✓ SEP - NOV 2023
OMB OIRA reviews proposed rule.

✓ DEC 26, 2023
Proposed rule publishes to the Federal Register.

✓ DEC 26, 2023 - FEB 26, 2024
60 day proposed rule public comment period.

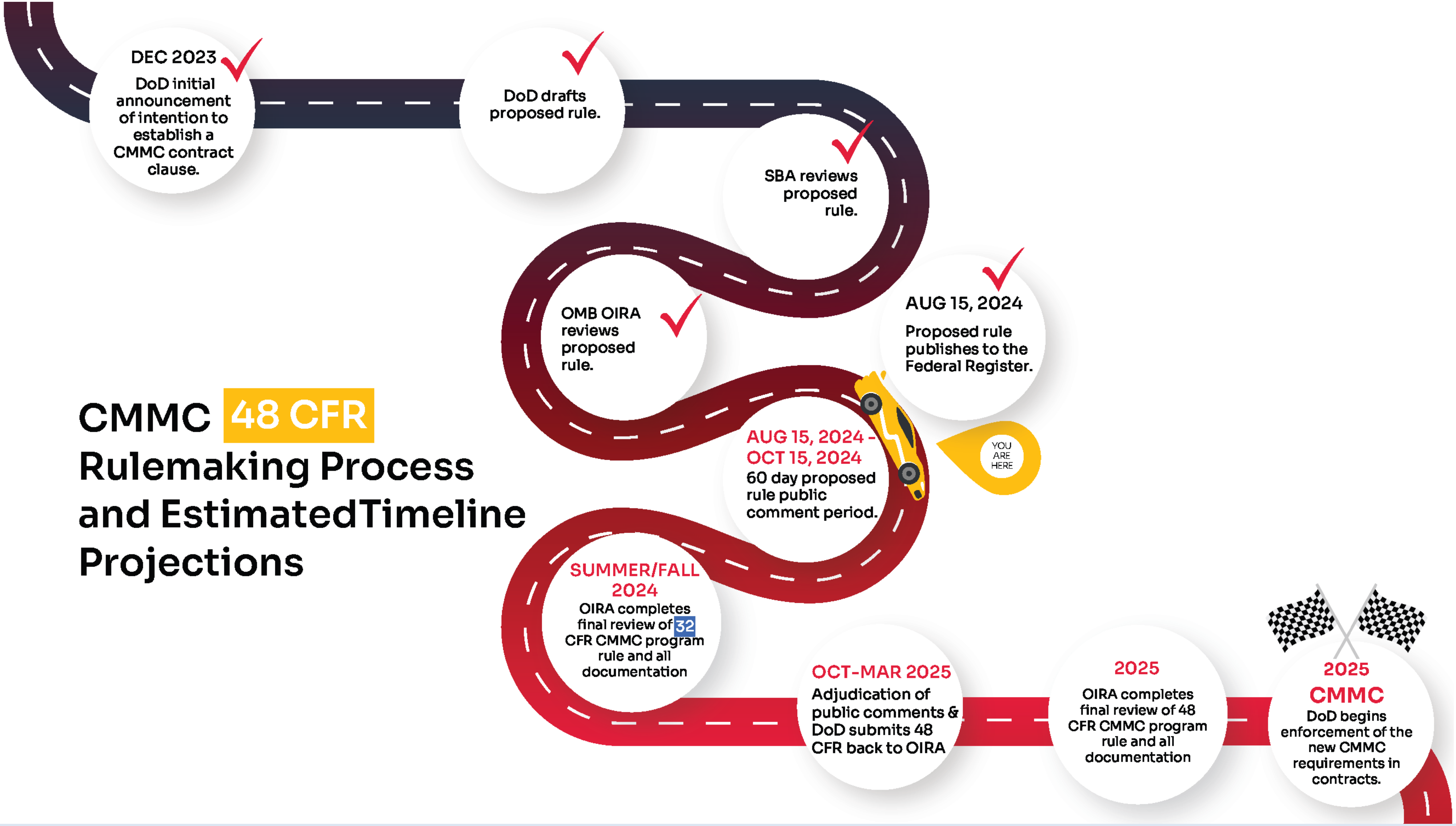
✓ FEB-JUN 2024
Adjudication of public comments & DoD submits 32 CFR to OIRA

✓ AUG 15, 2024
Release of 48 CFR CMMC proposed Rule

SUMMER/FALL 2024
OIRA completes final review of 32 CFR CMMC program rule and all documentation

2025
CMMC
Becomes final & implemented as a requirement attesting to NIST compliance

CFR 48 Timeline



CMMC 48 CFR Rulemaking Process and EstimatedTimeline Projections

DEC 2023 ✓
DoD initial announcement of intention to establish a CMMC contract clause.

✓ DoD drafts proposed rule.

✓ SBA reviews proposed rule.

OMB OIRA reviews proposed rule. ✓

✓ AUG 15, 2024
Proposed rule publishes to the Federal Register.

AUG 15, 2024 - OCT 15, 2024
60 day proposed rule public comment period.

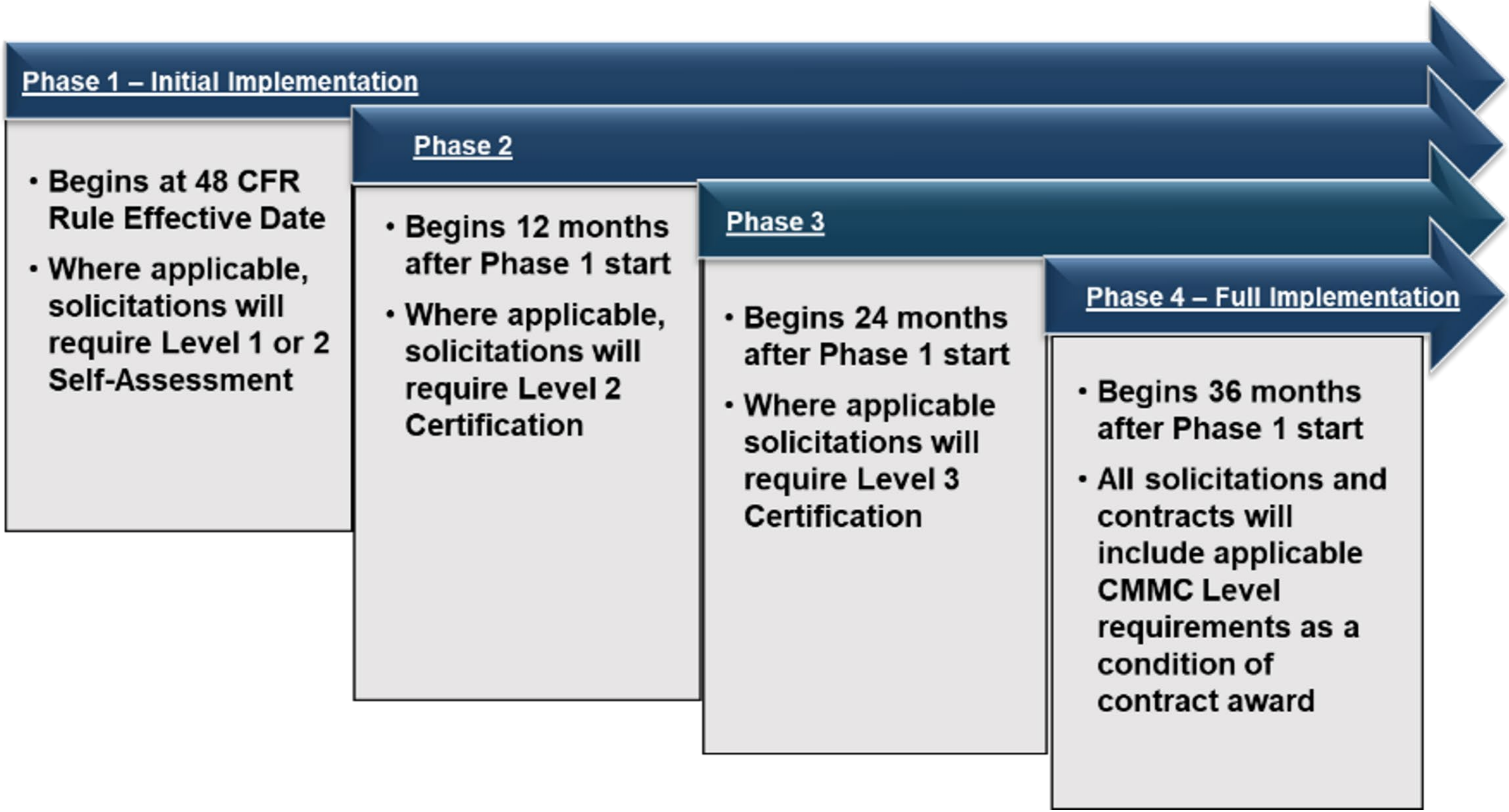
SUMMER/FALL 2024
OIRA completes final review of 32 CFR CMMC program rule and all documentation

OCT-MAR 2025
Adjudication of public comments & DoD submits 48 CFR back to OIRA

2025
OIRA completes final review of 48 CFR CMMC program rule and all documentation

2025
CMMC
DoD begins enforcement of the new CMMC requirements in contracts.

CFR 48 Timeline (Continued)



Phase 1 – Initial Implementation

- Begins at 48 CFR Rule Effective Date
- Where applicable, solicitations will require Level 1 or 2 Self-Assessment

Phase 2

- Begins 12 months after Phase 1 start
- Where applicable, solicitations will require Level 2 Certification

Phase 3

- Begins 24 months after Phase 1 start
- Where applicable solicitations will require Level 3 Certification

Phase 4 – Full Implementation

- Begins 36 months after Phase 1 start
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

Project Overview - Context

The CMMC Program provides assessments at three levels, each incorporating security requirements from existing regulations and guidelines.

Level 1: Basic Safeguarding of FCI

- **Requirements:**
  - Annual self-assessment and annual affirmation of compliance with the 15 security requirements in FAR clause 52.204-21.

Level 2: Broad Protection of CUI

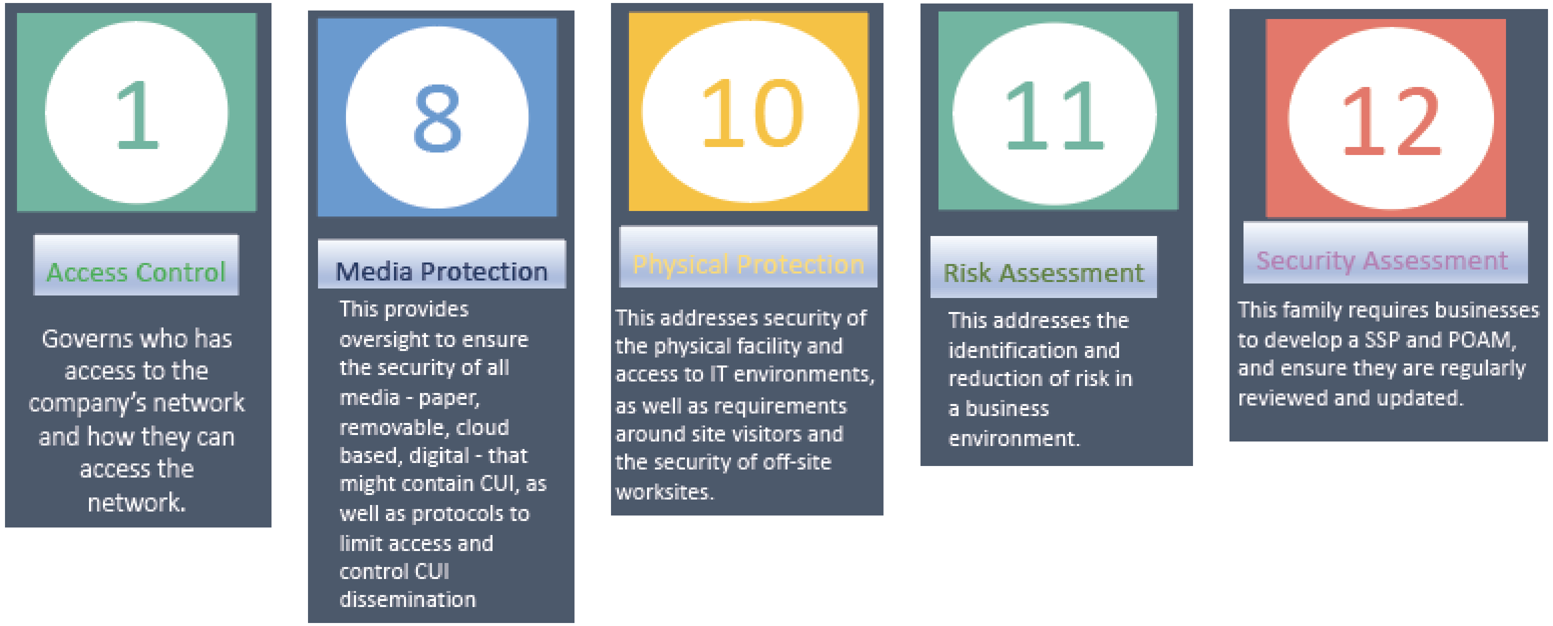
- **Requirements**:
  - Either a self-assessment or a C3PAO assessment every three years, as specified in the solicitation.
  - Decided by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems.
  - Annual affirmation, verify compliance with the 110 security requirements in NIST SP 800-171 Revision 2.

Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats

- **Requirements**:
  - Achieve CMMC Status of Final Level 2.
  - Undergo an assessment every three years by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).
  - Provide an annual affirmation verifying compliance with the 24 identified requirements from NIST SP 800-172.

Background: NIST SP 800-171

Example of Control Descriptions



1

Access Control

Governs who has access to the company's network and how they can access the network.

8

Media Protection

This provides oversight to ensure the security of all media - paper, removable, cloud based, digital - that might contain CUI, as well as protocols to limit access and control CUI dissemination

10

Physical Protection

This addresses security of the physical facility and access to IT environments, as well as requirements around site visitors and the security of off-site worksites.

11

Risk Assessment

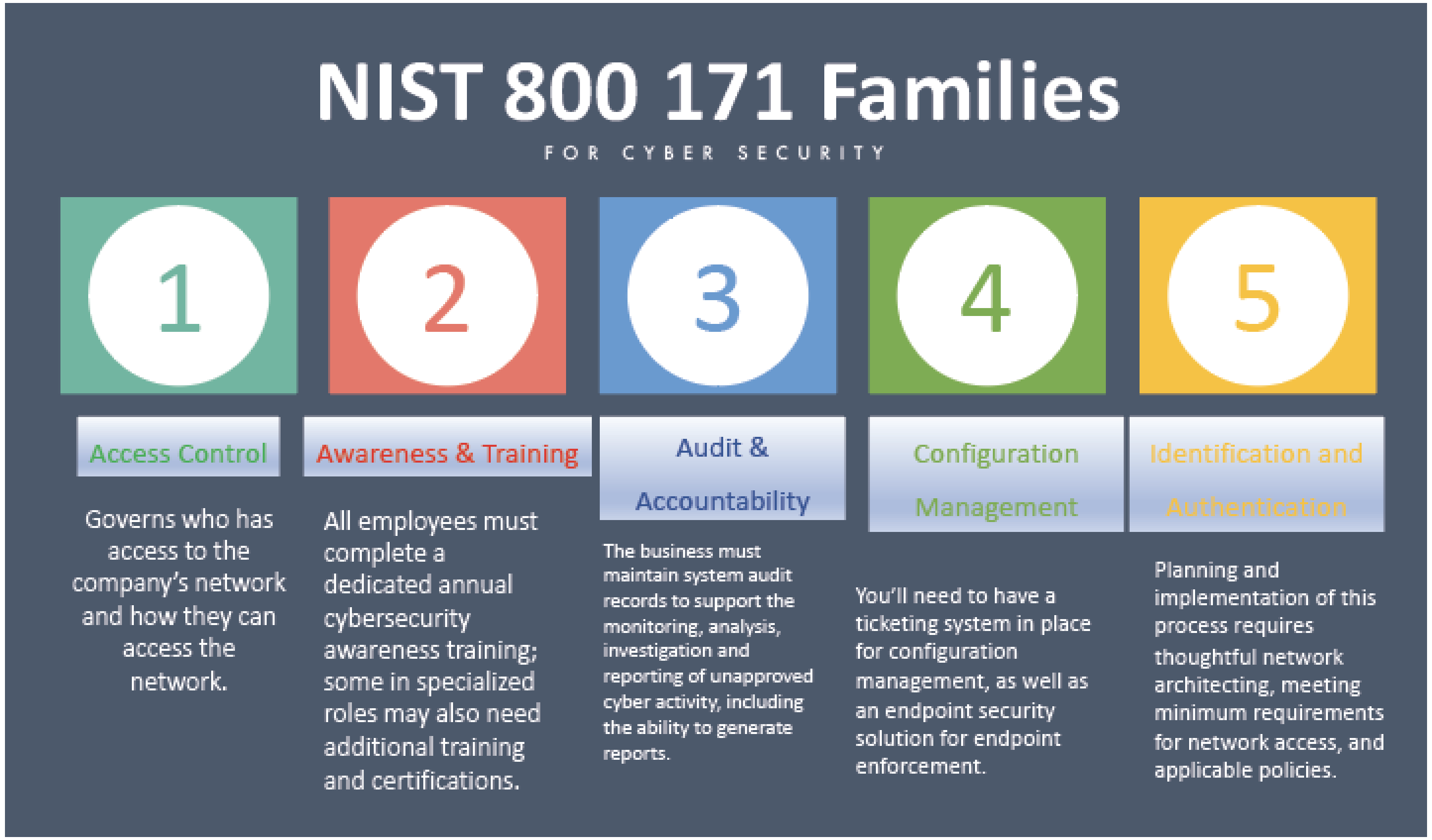
This addresses the identification and reduction of risk in a business environment.

12

Security Assessment

This family requires businesses to develop a SSP and POAM, and ensure they are regularly reviewed and updated.

The goal is to checkmark these 14 control families over the course of the program



NIST 800 171 Families

FOR CYBER SECURITY

1 Access Control

Governs who has access to the company's network and how they can access the network.

2 Awareness & Training

All employees must complete a dedicated annual cybersecurity awareness training; some in specialized roles may also need additional training and certifications.

3 Audit & Accountability

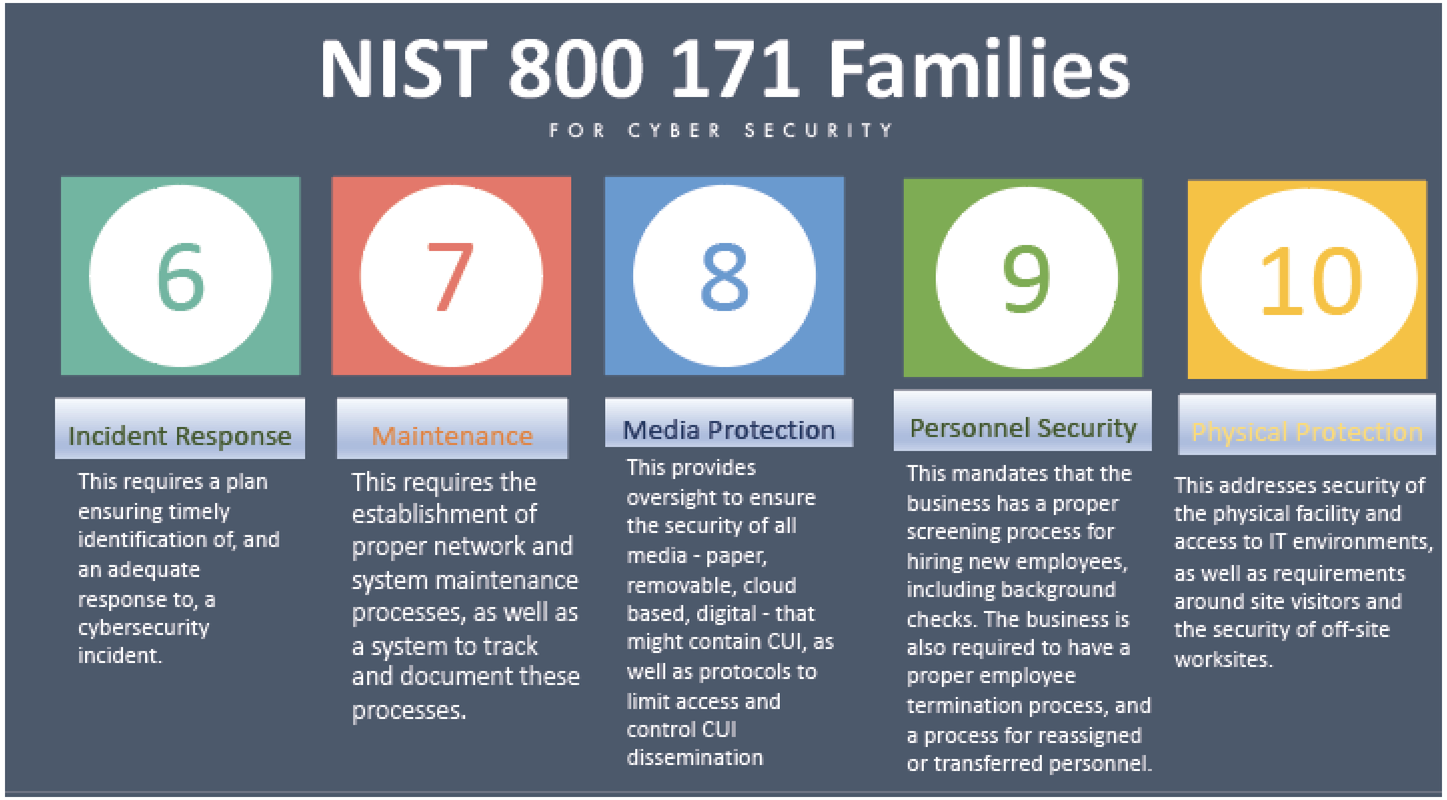
The business must maintain system audit records to support the monitoring, analysis, investigation and reporting of unapproved cyber activity, including the ability to generate reports.

4 Configuration Management

You'll need to have a ticketing system in place for configuration management, as well as an endpoint security solution for endpoint enforcement.

5 Identification and Authentication

Planning and implementation of this process requires thoughtful network architecting, meeting minimum requirements for network access, and applicable policies.



NIST 800 171 Families

FOR CYBER SECURITY

6

Incident Response

This requires a plan ensuring timely identification of, and an adequate response to, a cybersecurity incident.

7

Maintenance

This requires the establishment of proper network and system maintenance processes, as well as a system to track and document these processes.

8

Media Protection

This provides oversight to ensure the security of all media - paper, removable, cloud based, digital - that might contain CUI, as well as protocols to limit access and control CUI dissemination

9

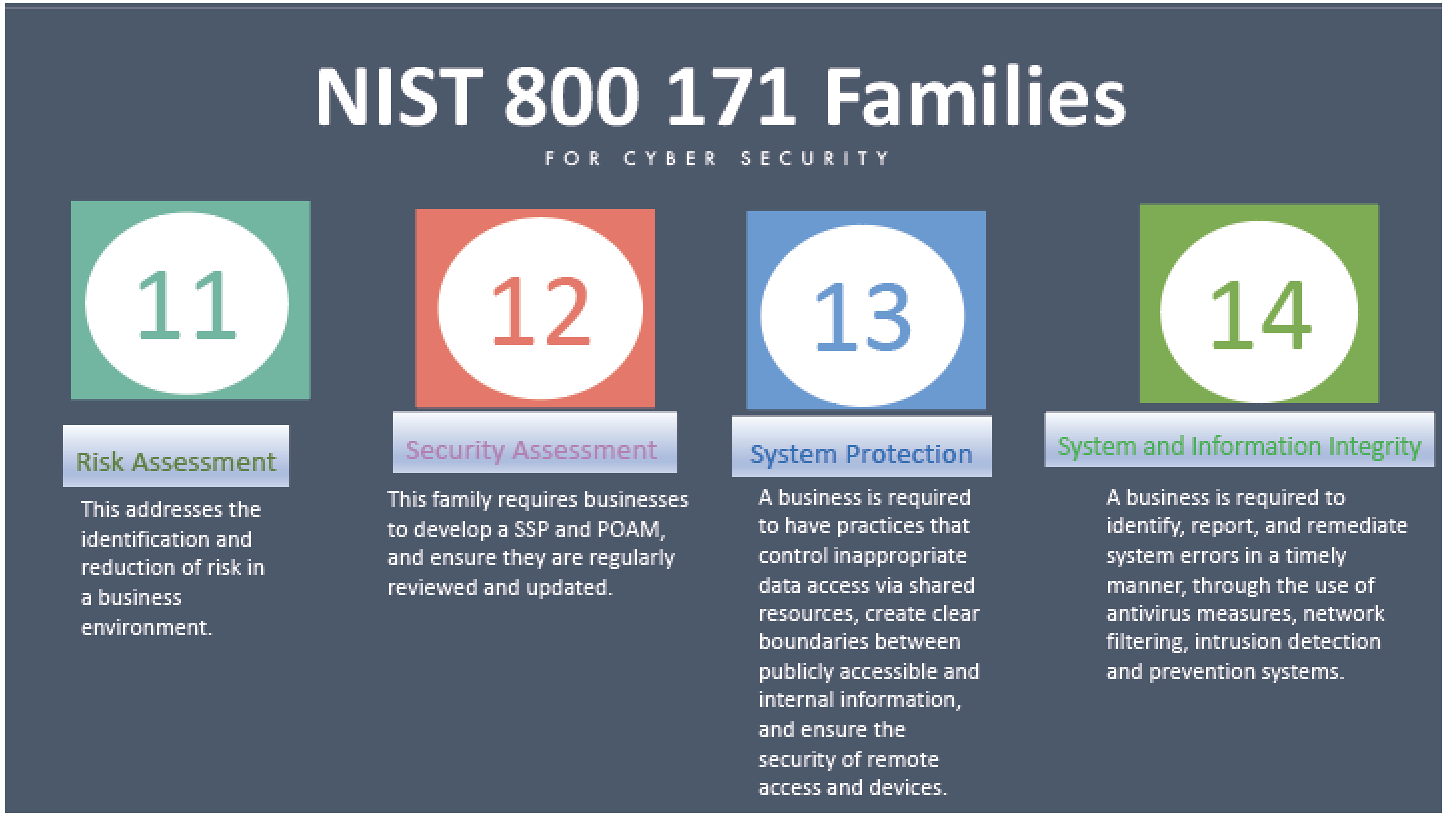
Personnel Security

This mandates that the business has a proper screening process for hiring new employees, including background checks. The business is also required to have a proper employee termination process, and a process for reassigned or transferred personnel.

10

Physical Protection

This addresses security of the physical facility and access to IT environments, as well as requirements around site visitors and the security of off-site worksites.



NIST 800 171 Families

FOR CYBER SECURITY

11

Risk Assessment

This addresses the identification and reduction of risk in a business environment.

12

Security Assessment

This family requires businesses to develop a SSP and POAM, and ensure they are regularly reviewed and updated.

13

System Protection

A business is required to have practices that control inappropriate data access via shared resources, create clear boundaries between publicly accessible and internal information, and ensure the security of remote access and devices.

14

System and Information Integrity

A business is required to identify, report, and remediate system errors in a timely manner, through the use of antivirus measures, network filtering, intrusion detection and prevention systems.

United Rotorcraft®

7301 S Peoria St. | Englewood, CO 80112 | (303) 792-7400
www.unitedrotorcraft.com