United Rotorcraft

Supplier CMMC Readiness

January 23, 2025

Agenda

- Introductions
- Fundamental Questions
- Background
- Project Overview
- Questions?
- References

Introductions

United Rotorcraft®

- Carlos Hernandez
  Contracts Admin & CX Services Mgr.
- Mike Kingzett
  Sr Dir of Business Transformation
- 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

Fundamental Questions

What is CMMC?
- CMMC stands for Cybersecurity Maturity Model Certification.

What is CMMC's purpose?
- Protect sensitive information

What is the United Rotorcraft (UR) and Manufacturer's Edge (ME) Partnership Purpose?
- Identify cybersecurity status with today's existing DFARS
- Achieve CMMC readiness

Why is this significant to our business?
- CMMC became law on December 16, 2024, per CFR 32
- The collaborative effort program will ensure we aim
  - Compliancy with existing DFARS and upcoming CMMC requirements
  - Business continuity
  - Avoiding legal fees, fines, including False Claims Act (FCA)

Position suppliers for success by achieving CMMC readiness for business continuity

Background: CUI & DFARS

- **Early-mid 2000s**
  - The need to protect sensitive Government data traces back to the 9/11 Commission Report
- **2010**
  - Executive Order 13556 – Creation of Controlled Unclassified Information (CUI) program was established
- **2015**
  - NIST SP 800-171 was released, a framework to apply for safeguarding CUI data
- **2016**
  - A regulation was issued establishing a policy for Federal agencies on the designation, safeguarding, dissemination, and marking of CUI
- **2017**
  - DFARS regulations went into effect to protect Covered Defense Information (CDI) including CUI.
- **2020-Present**
  - DFARS introduced regarding SPRS reporting and flow down requirement

Takeaways

- 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
- DFARS 252.204-7021 (2025) → 3rd Party CMMC certification

Background: NIST SP 800-171

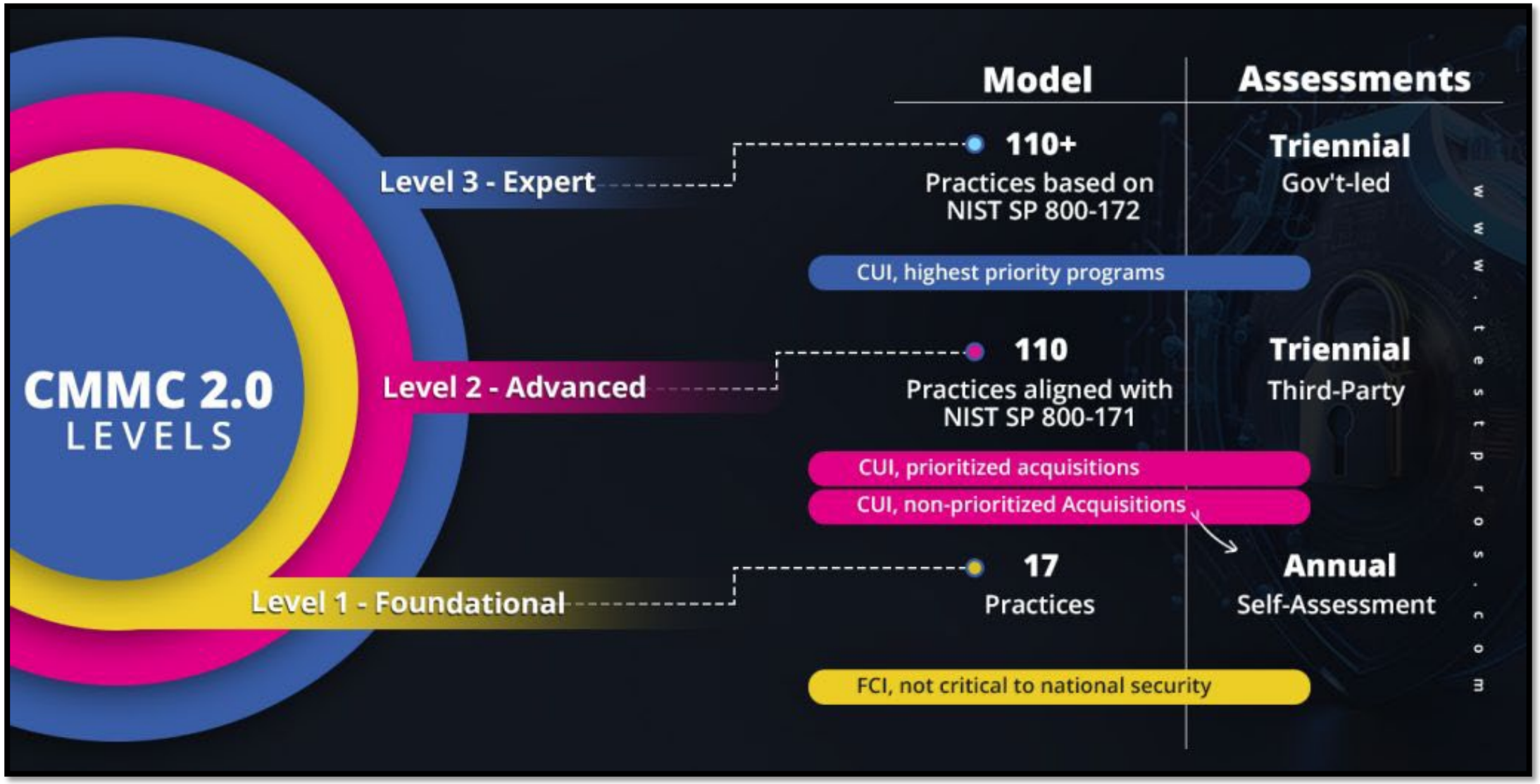
14 Control Families

Background: NIST SP 800-171

110 Controls

	AC	AT	AU	CM	IA	IR	MA	MP	PS	PE	RA	CA	SC	SI
Basic (FIPS 200)	3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
	3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
								3.8.3			3.11.3	3.12.3		3.14.3
												(3.12.4)		
Derived (800-53)	3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.4		3.10.3			3.13.3	3.14.4
	3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.5		3.10.4			3.13.4	3.14.5
	3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.6		3.10.5			3.13.5	3.14.6
	3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.7		3.10.6			3.13.6	3.14.7
	3.1.7		3.3.7	3.4.7	3.5.7			3.8.8					3.13.7	
	3.1.8		3.3.8	3.4.8	3.5.8			3.8.9					3.13.8	
	3.1.9		3.3.9	3.4.9	3.5.9								3.13.9	
	3.1.10				3.5.10								3.13.10	
	3.1.11				3.5.11								3.13.11	
	3.1.12												3.13.12	
	3.1.13												3.13.13	
	3.1.14												3.13.14	
	3.1.15				Policy/Process			Policy or Software Requirement					3.13.15	
	3.1.16												3.13.16	
	3.1.17				Configuration			Configuration or Software						
	3.1.18													
	3.1.19				Software			Configuration or Software or Hardware						
	3.1.20													
	3.1.21				Hardware			Software or Hardware						
	3.1.22													

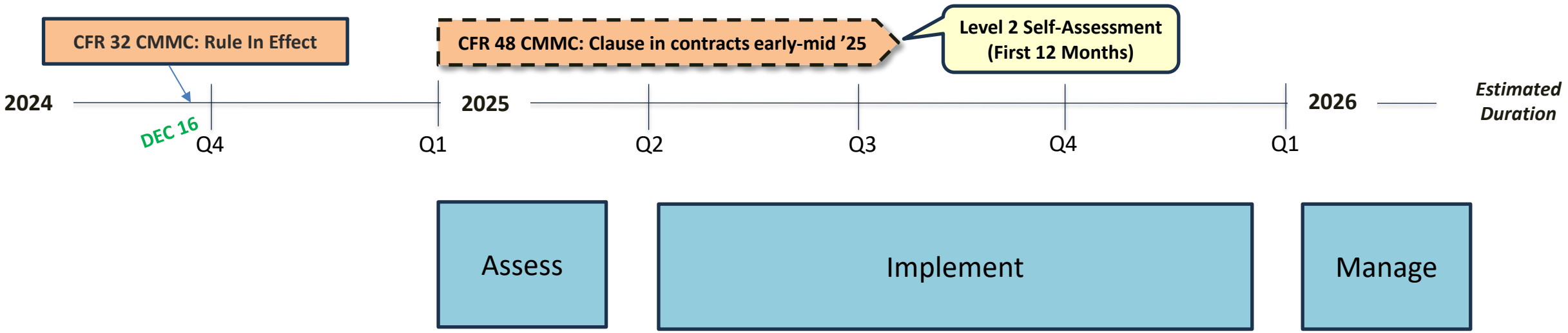
Background: CMMC 2.0



Project Overview - Approach

Phase	Key Deliverables	Key Objective
1 Phase 0: Supplier Education Event	▪ Understanding of the requirements and the importance of business continuity	Assess
2 Phase 1: Gap Analysis	▪ Informs individual scorecard ▪ Customized program ▪ Timeline for compliance	
3 Phase 2: Implementation	▪ Create an SSP ▪ Develop POA&M ▪ Develop Timeline for completion	Implement
4 Phase 3: Supplier Assessment	▪ Risk mitigation and planning ▪ Update scorecard and report affirmations to SPRS	
5 Phase 4: Compliance Assessment	▪ Final Assessment – supplier scorecard indicating likelihood of compliance within timeline	Manage
6 Phase 5: Maint & Ongoing Compliance	▪ Ensure SOPs for all suppliers related to ongoing requirements to maintain CMMC-level compliance	

Project Overview – Timeline



Questions?

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

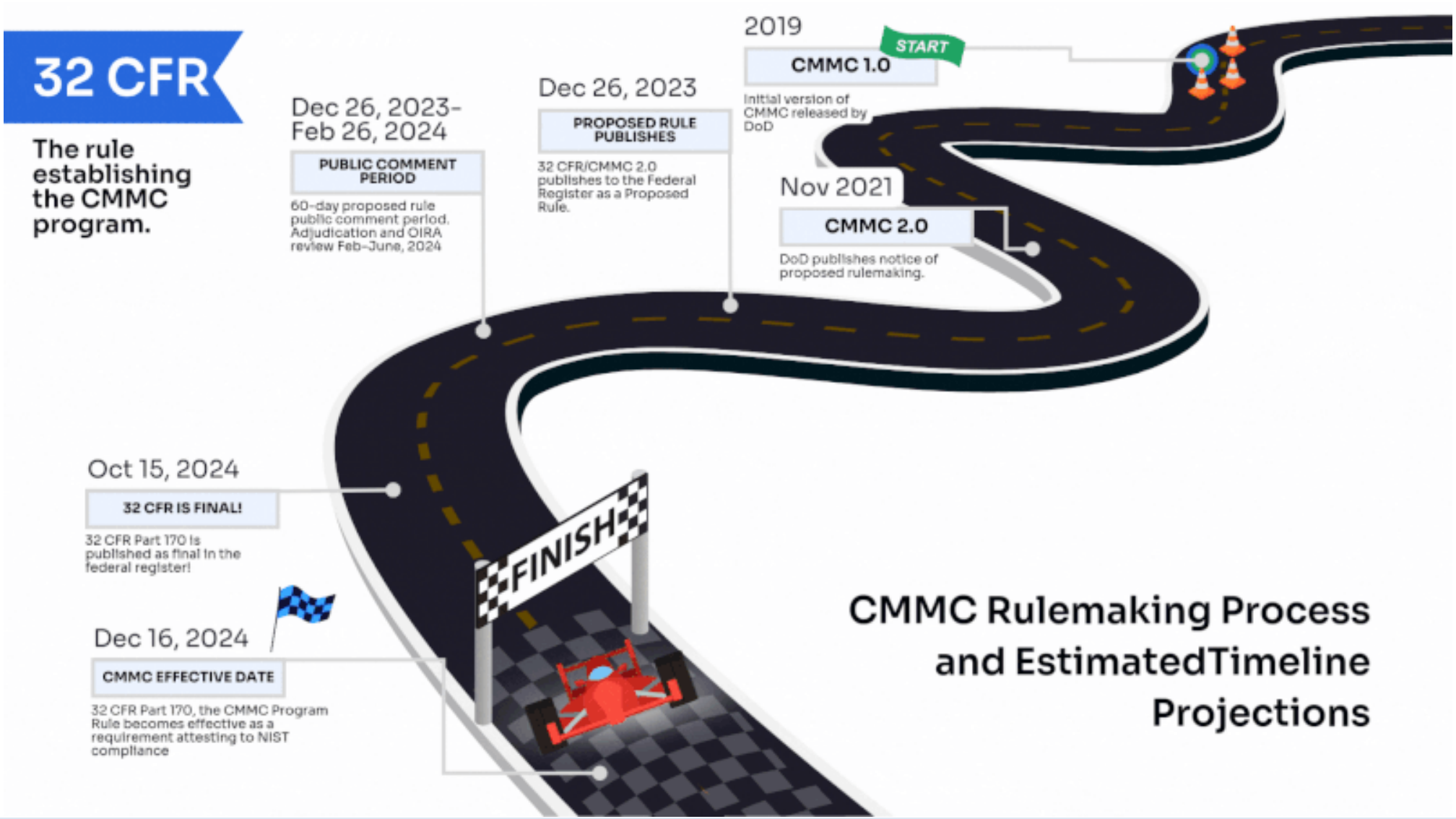
NIST SP 800-171 vs NIST 800-53

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

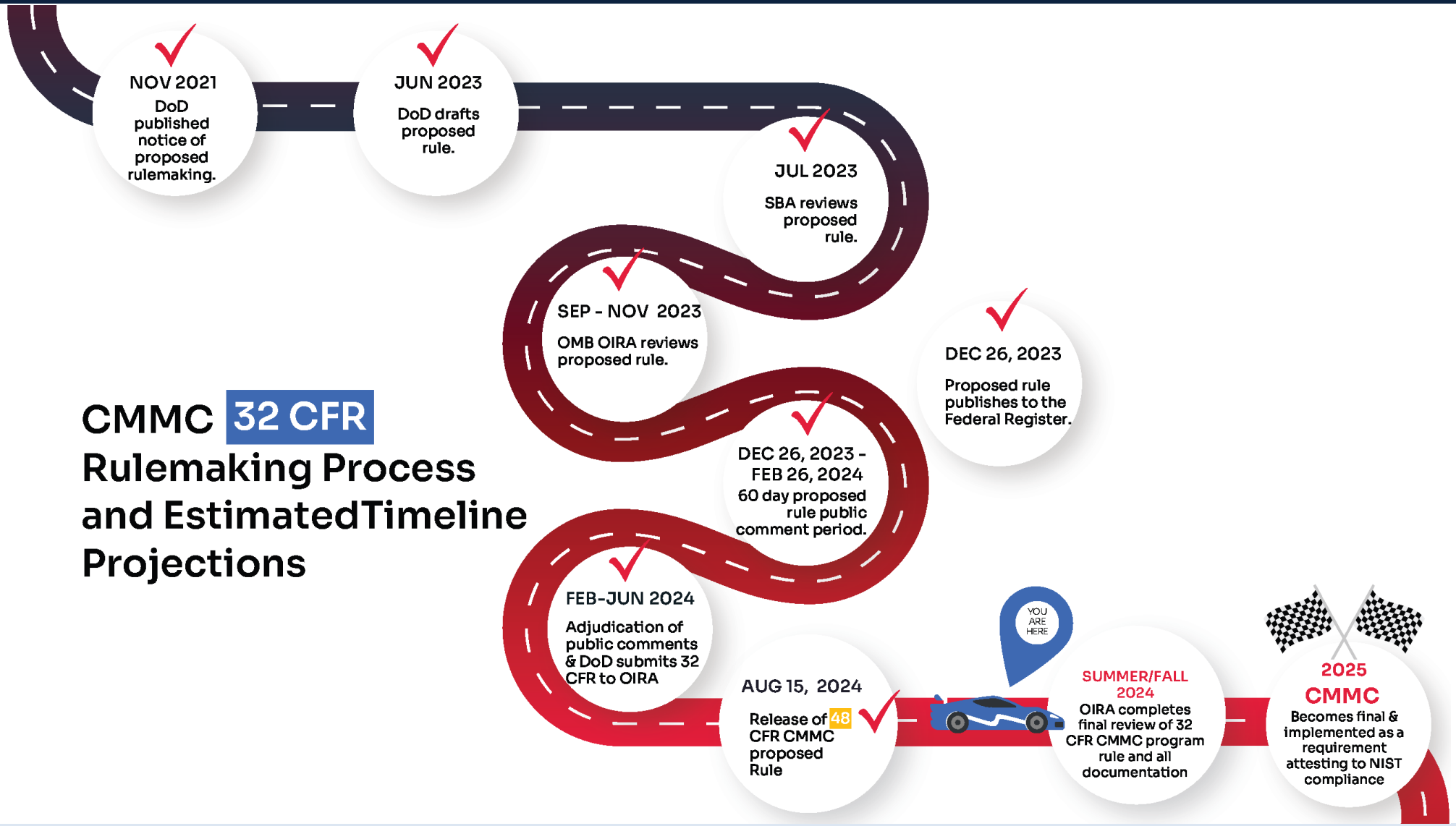
Code of Federal Regulations (CFR)

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

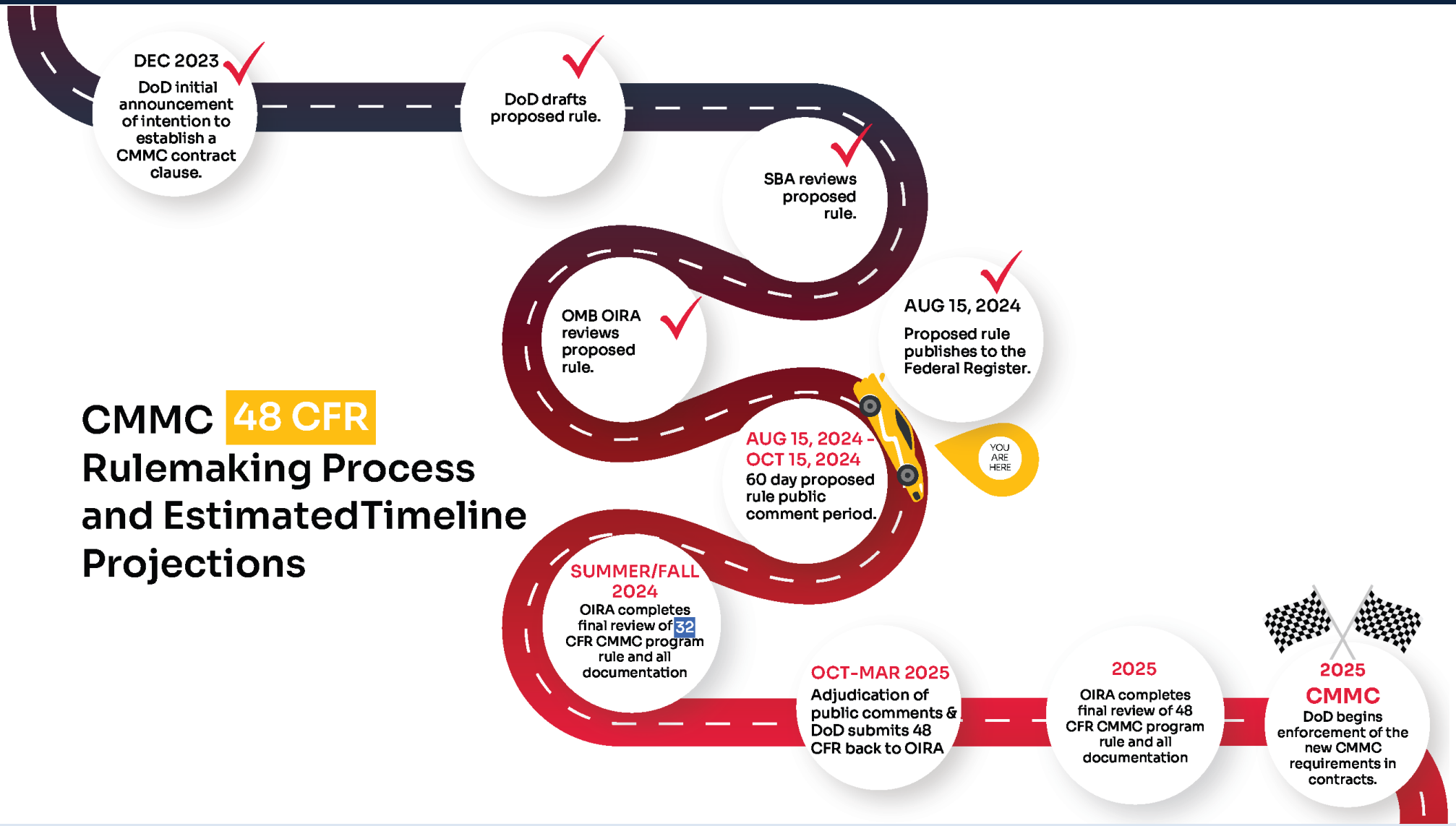


CFR 32 Timeline



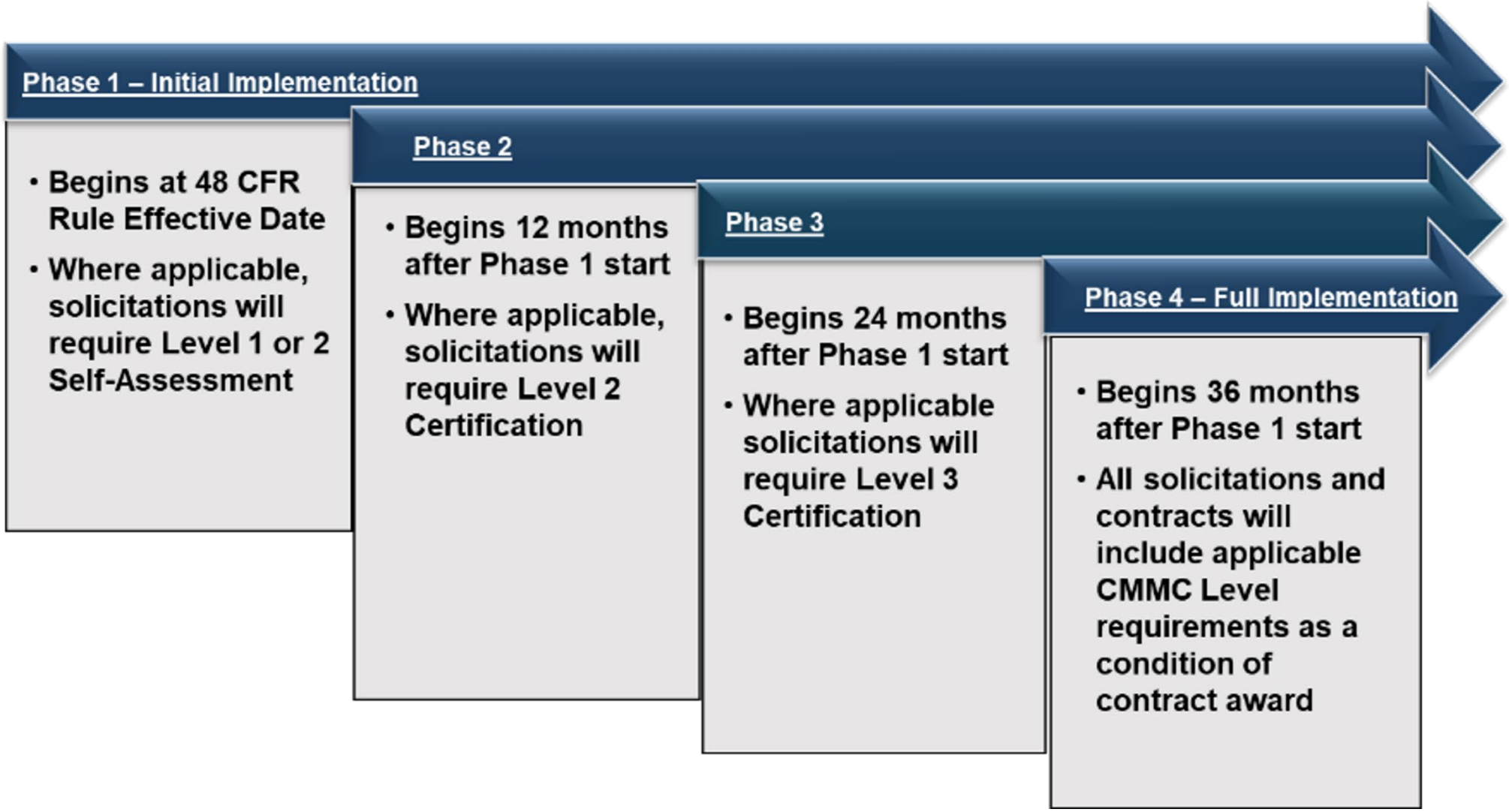
CMMC 32 CFR Rulemaking Process and EstimatedTimeline Projections

CFR 48 Timeline



CMMC 48 CFR Rulemaking Process and EstimatedTimeline Projections

CFR 48 Timeline (Continued)



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

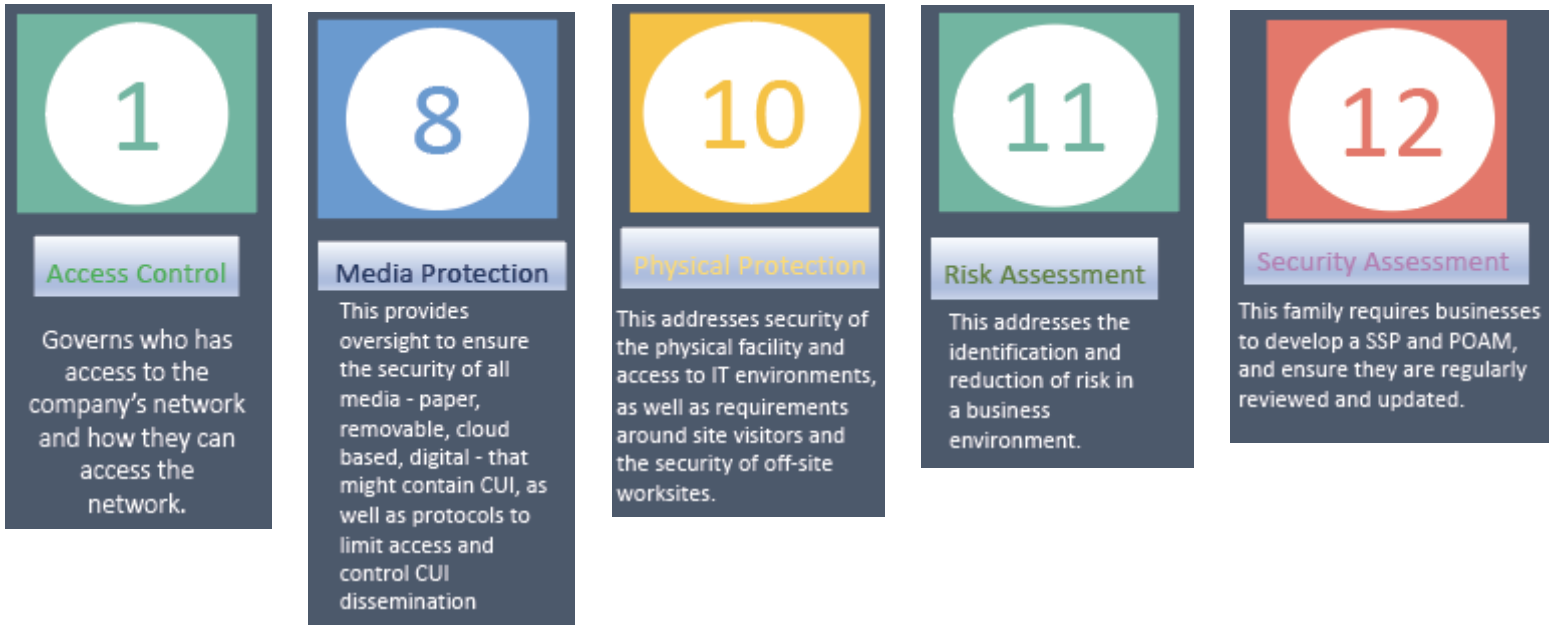
- **Requirements**:
  - Either a self-assessment or a C3PAO assessment every three years, as specified in the solicitation.
  - Decided by the type of information processed, transmitted, or stored on the contractor or subcontractor information systems.
  - Annual affirmation, verify compliance with the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

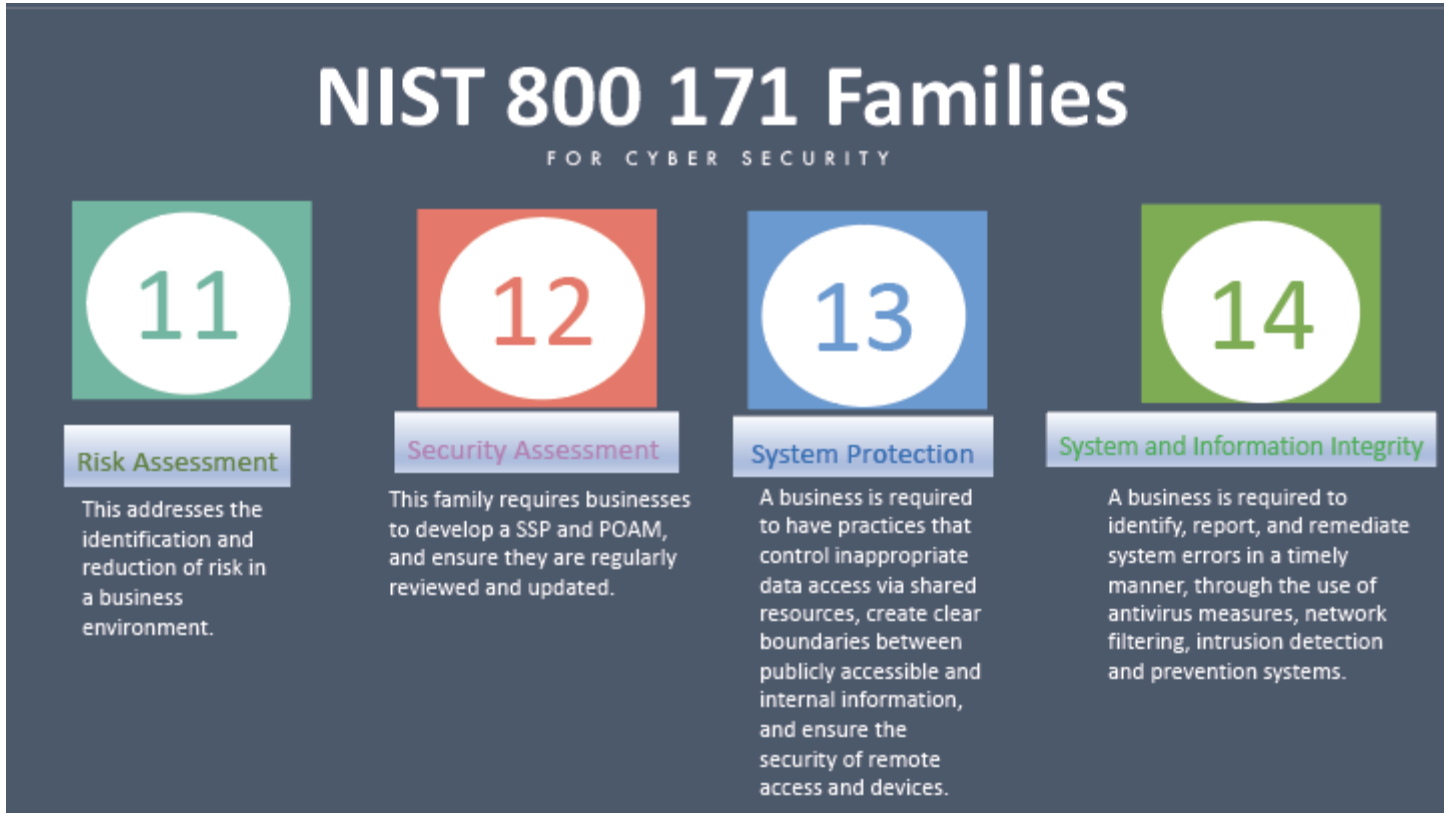
Example of Control Descriptions



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


NIST 800 171 Families
FOR CYBER SECURITY
1
2
3
4
5
Access Control
Awareness & Training
Audit & Accountability
Configuration Management
Identification and Authentication
Governs who has access to the company's network and how they can access the network.
All employees must complete a dedicated annual cybersecurity awareness training; some in specialized roles may also need additional training and certifications.
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.
You'll need to have a ticketing system in place for configuration management, as well as an endpoint security solution for endpoint enforcement.
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