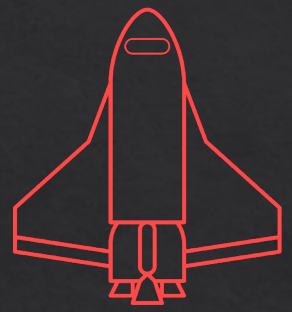


Space Coast Cyber

Comparing Risk Management Framework (RMF) and Cybersecurity Maturity Model Certification (CMMC)

ISSA-NOVA

10/19/2023

Dr. Jeff Baldwin, CISSP-ISSAP-ISSEP, CCSP, CISM, CISA, PMP

CMMC Provisional Instructor / Certified CMMC Assessor

Founder & CEO, Space Coast Cyber

Speaker Introduction

- My least favorite slide – but it is good to know your biases
- Earned Doctor of Science in Cybersecurity, MS in Information Assurance, and BTech in IT Network Administration
- Both a practitioner (17+ years) and an educator (professor for 13+ years)
- Worked with NIST SP 800-53 since initial release in 2005.
- As a Security Control Assessor, I have formally assessed over 150 systems
- As an Information Systems Security Engineer, I have self-assessed over 100 systems which led to a successful Authority to Operate (ATO)
- CMMC Provisional Instructor / Licensed Training Provider
- CMMC Consultant and Program Manager
- LinkedIn: https://www.linkedin.com/in/drjeffbaldwin/

Agenda

- My Career Journey
- Key Terms
- DFARS 7012, NIST SP 800-171
- 5 W's of CMMC
- RMF Comparison to CMMC
- Key Similarities and Differences
- Career Opportunities
- Closing Thoughts
- Q&A

My Career Journey

- Began infosec career as an Intern at the Department of Energy (contractor)
  - My first week: here's a stack of regulations to read (FISMA, OMB A-130, NIST SP 800-53, 800-37, 800-30, FIPS 199, FIPS 200)
- Graduated and worked at Battelle (thanks for hosting tonight's event!)
- Tried out Government Service: Defense Security Service and NIST
- Ventured back into contracting within the Intelligence Community
- Migrated to Florida and worked for L3Harris (why wait until retirement?)
- COVID-19 happened and did not want to work onsite anymore
- Found remote job with L3Harris within Supply Chain Cybersecurity
- Started side gig as a CMMC Trainer
- Now full-time CMMC Program Manager, Consultant, and Assessor

Key Terms

- **Information System** - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- **System Component** - A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.
- Federal Acquisition Regulation (FAR) 52.204-21 *Basic Safeguarding of Covered Contractor Information Systems.*
- Security Domain - A domain that implements a security policy and is administered by a single authority.
- **FCI** – Federal Contract Information
- **CUI** – Controlled Unclassified Information
- **OSC** – Organization Seeking Certification
- **C3PAO** – CMMC Third Party Assessment Organization

DFARS 7012

- Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting.*
- "**Covered contractor information system**" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.
  - Does not include systems operated on behalf of the government.
- "Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is
  - (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
  - (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.
- Requires **NIST SP 800-171** for the safeguarding of CDI

NIST SP 800-171

- NIST SP 800-171 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
- **Tailored from the NIST SP 800-53 Moderate Baseline**
- Security Controls -> 110 Security Requirements -> 110 CMMC Practices
- 18 Control Families –> 14 Domains

TABLE E: TAILORING ACTION SYMBOLS

TAILORING SYMBOL	TAILORING CRITERIA
NCO	NOT DIRECTLY RELATED TO PROTECTING THE CONFIDENTIALITY OF CUI.
FED	UNIQUELY FEDERAL, PRIMARILY THE RESPONSIBILITY OF THE FEDERAL GOVERNMENT.
NFO	EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION.
CUI	THE CUI BASIC OR DERIVED SECURITY REQUIREMENT IS REFLECTED IN AND IS TRACEABLE TO THE SECURITY CONTROL, CONTROL ENHANCEMENT, OR SPECIFIC ELEMENTS OF THE CONTROL/ENHANCEMENT.

NIST SP 800-171 Scoping

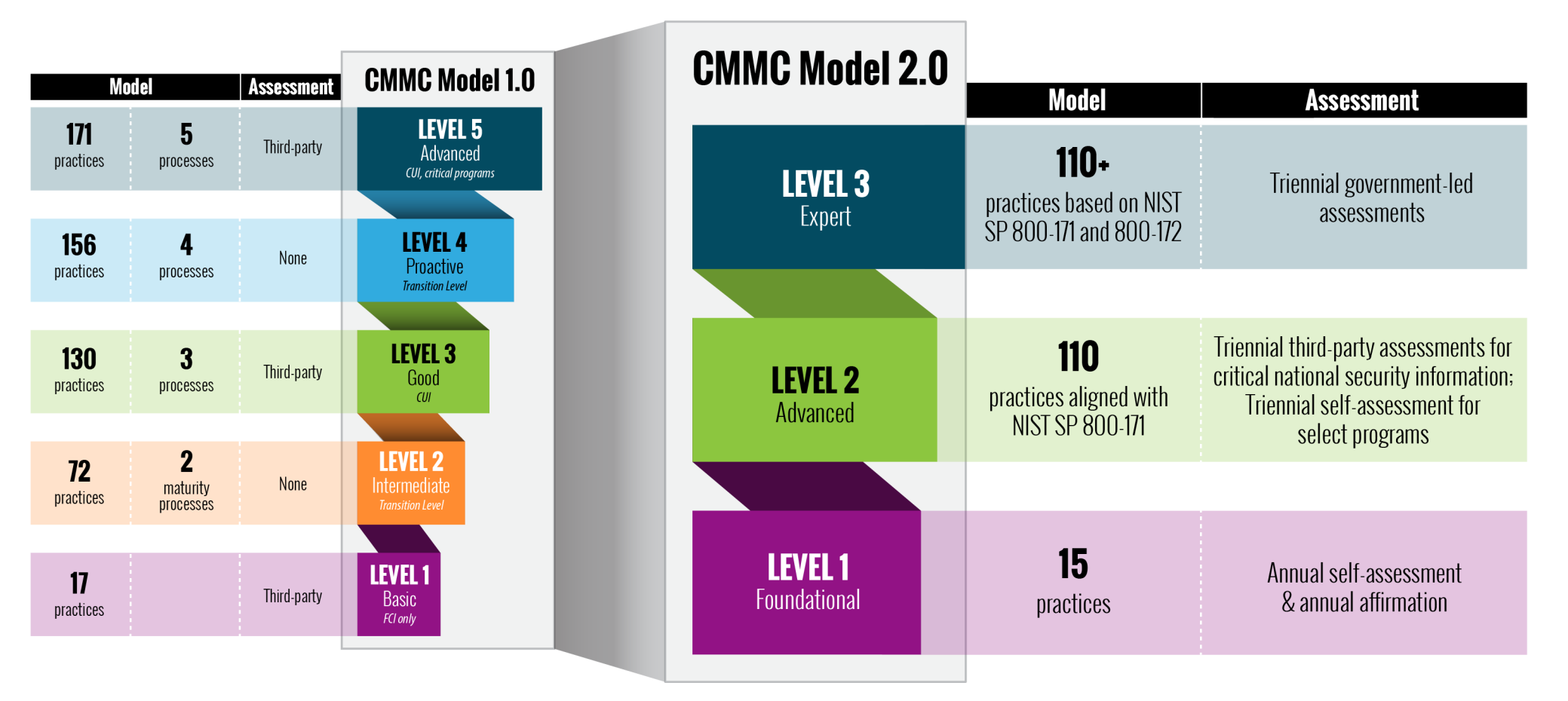
1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide federal agencies with recommended security requirements[6] for protecting the *confidentiality* of CUI: (1) when the CUI is resident in a nonfederal system and organization; (2) when the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency;[7] and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.[8]

The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.[9] If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI *security domain*. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.

Cybersecurity Maturity Model Certification

- Currently in the rulemaking process right now for new DFARS 7021 clause
- Third party assessment of NIST SP 800-171 requirements at Level 2



Why was CMMC created?

- DCMA's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) and the DoD IG found through assessments that the cybersecurity requirements of NIST SP 800-171 were not being performed by Defense Contractors
- CMMC assessments allow the Department to verify the implementation of cybersecurity requirements with a higher level of assurance than provided by Self-Assessments and Self-Attestations
- Primary goals of the CMMC 2.0 program:
  - Safeguard sensitive information to enable and protect the warfighter
  - Enforce DIB cybersecurity standards to meet evolving threats
  - Ensure accountability while minimizing barriers to compliance with DoD requirements
  - Perpetuate a collaborative culture of cybersecurity and cyber resilience
  - Maintain public trust through high professional and ethical standards (About CMMC, 2022)

Who created CMMC?

- Originally sponsored by the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)
- No cost contract established with the CMMC-AB, now known as The CyberAB to oversee accreditation of CMMC Third Party Assessment Organizations (C3PAOs)
- The CMMC Program Management Office transitioned to the DoD CIO

Where is CMMC intended?

- Requirements applied to Covered Contractor Information Systems
- **Data Driven**: Applies where FCI/CUI is Processed/Stored/Transmitted
- **Implementation through Contracts**: Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award (About CMMC, 2022)
- DFARS Case 2019-D041 introduced DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirements.
- Federal Contract Information (FCI) requires CMMC Level 1
- Controlled Unclassified Information (CUI) requires CMMC Level 2
- The highest priority, most critical defense programs will require CMMC Level 3

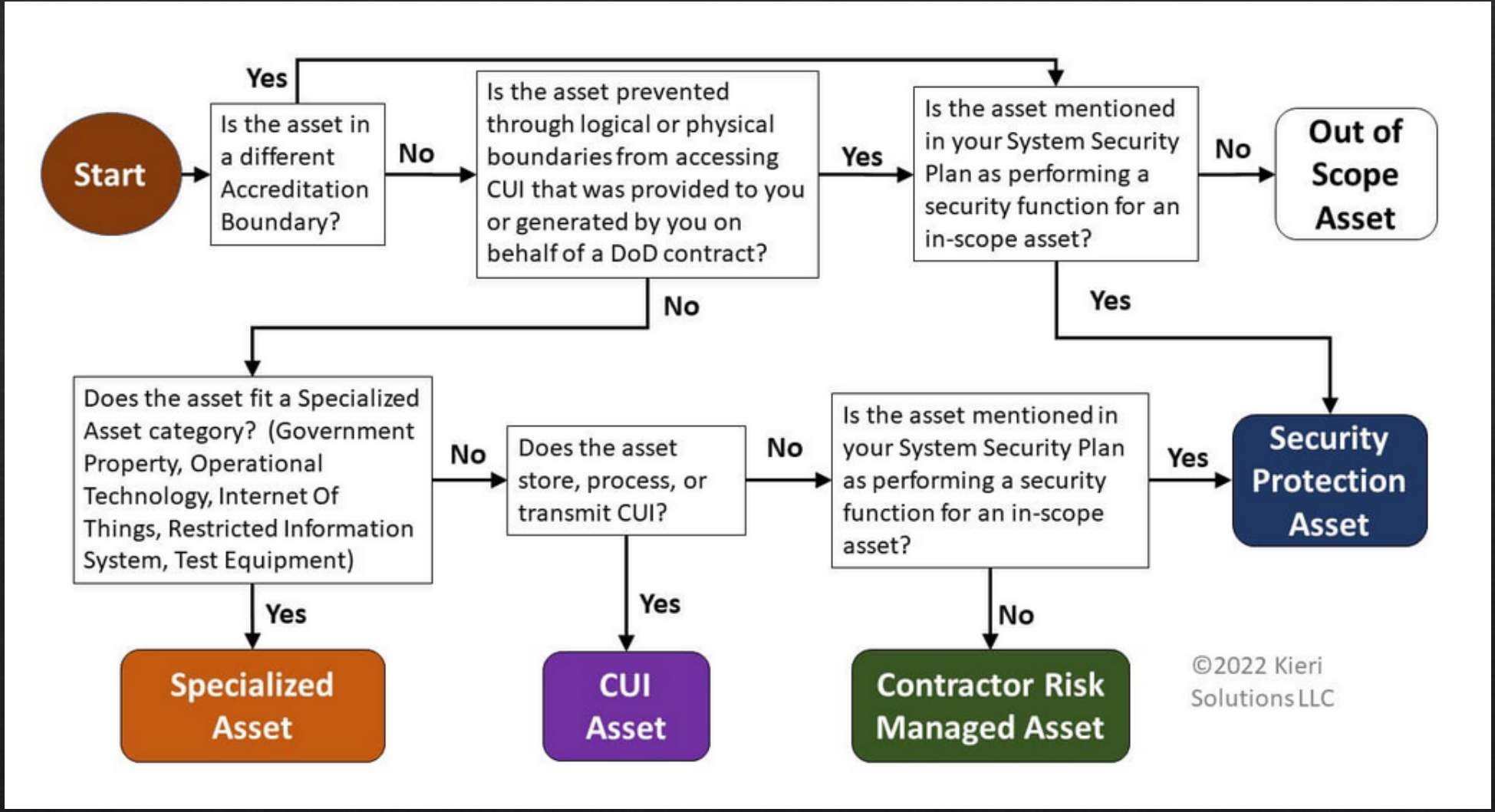
When is CMMC?

- The changes reflected in CMMC 2.0 will be implemented through the rulemaking process. **Companies will be required to comply once the forthcoming rules go into effect**. The Department intends to pursue rulemaking both in Part 32 of the Code of Federal Regulations (C.F.R.) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the C.F.R. (About CMMC, 2022)
- Estimated Fall 2023 for rulemaking. Basically, any day now.
- CMMC 2.0 will become a contract requirement once rulemaking is completed.
  - Interim Final Rule – in effect in 60 days
  - Proposed Rule – adds roughly another 12 months to the timeline
- In FY 2025 or CY 2025, I would expect to see 7021 clause in some DoD contracts

CMMC Scoping

- **Out-of-Scope Assets**
  - Assets that cannot process, store, or transmit CUI
- **Specialized Assets**
  - Assets that may or may not process, store, or transmit CUI
  - Assets include government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment
- **Contractor Risk Managed Assets**
  - Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place
  - Assets are not required to be physically or logically separated from CUI assets
- **Security Protection Assets**
  - Assets that provide security functions or capabilities to the contractor's CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI
- **Controlled Unclassified Information (CUI) Assets**
  - Assets that process, store, or transmit CU

CMMC Scoping



- https://www.cmmcaudit.org/cmmc-2-0-scoping-scenarios-analysis/

NIST SP 800-53

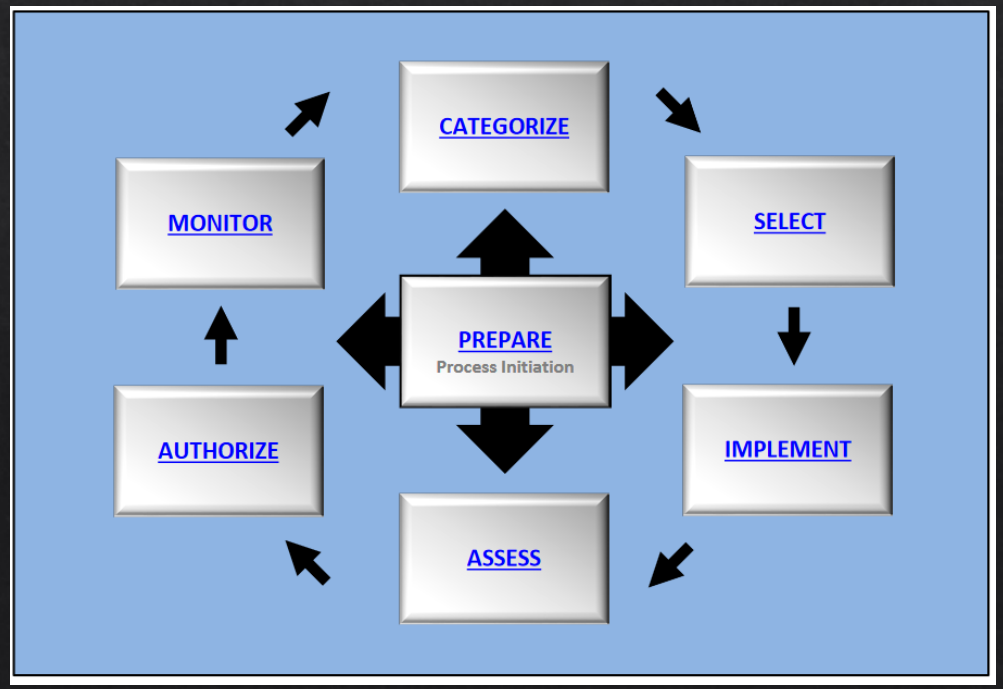
- NIST Special Publication 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations*
- All roads lead back to NIST SP 800-53, current revision is Rev. 5
- Catalog of hundreds of security controls and control enhancements
- Applies to **Federal Information Systems**, or **systems operated on behalf of government agencies**.

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

NIST SP 800-37 RMF

- NIST Special Publication 800-37 Rev. 2 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- Security Authorization process followed for Federal Information Systems, or Systems Operated on Behalf of Government Agencies



RMF Comparison to CMMC

RMF	CMMC
0 – Prepare	OSC Prepares for Certification
1 – Categorize [FIPS 199, NIST SP 800-60]	Contracts - FCI (Level 1) or CUI (Level 2+) [FIPS 199]
2 – Select [NIST SP 800-53B]	CMMC Model Levels [FAR, NIST SP 800-171, NIST SP 800-172]
3 – Implement	OSC Implement Practices
4 – **Assess** [NIST SP 800-53A]	**CMMC Assessment Process (CAP)** [NIST SP 800-171A]
5 – Authorize Authority to Operate (ATO)	C3PAO issues CMMC certification
6 – Monitor	OSC monitors controls - 3.12.3

- 3.12.3 - Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls

CMMC Assessment Process

RMF	CAP
4 – Assess	Phase 1 – Plan and Prepare the Assessment Phase 2 – Conduct the Assessment
5 – Authorize	Phase 3 – Report Recommended Assessment Results Phase 4 – Close-out POA&Ms and Assessment
6 – Monitor	3-year C3PAO assessment cycle

- CMMC focuses on assessment but functionally overlaps between Step 4 and 5.
- CAP: https://cyberab.org/Portals/0/Documents/Process-Documents/CMMC-Assessment-Process-CAP-v1.0.pdf

Key Similarities

- Both are data driven, where the protection requirements follow the data
- Understanding your data flow can help manage the scope and system boundaries
- Both follow the concept of system boundaries and have System Security Plans (SSPs) that correspond to the system boundaries
- RMF and CMMC include an assessment against a standard created by NIST, 800-53 for RMF vs 800-171 & 800-172 for CMMC
- NIST SP 800-171 is derived from NIST SP 800-53
- CMMC Domains are Control Families
- Security Control Assessors (SCA) are similar to Certified CMMC Assessors (CCA), both review what is described and verify and validate the implementation as described

Key Differences

- RMF focuses on the management of risk and allows for Authorizing Officials (AOs) to accept risk and issue Authority to Operate (ATO)
- CMMC is a conformity assessment to a minimum standard with minimal ability for risk acceptance
  - Caveat: DoD Assessment Methodology (DoDAM) allows for temporary deficiencies and isolated enduring exceptions, but it is unclear if this will carryover to CMMC
- SCA for RMF usually have labor category requirements to meet
- Certified CMMC Assessors are required to attend training and complete CyberAB certifications – there is no self-study option
- C3PAOs issue certifications, AOs issue ATOs
- You can pick which C3PAO assesses you; with RMF you do not get a choice who assesses you, in most cases

Career Opportunities

- Implementer - Work directly for an Organization Seeking Certification (OSC), technical skills and/or documentation skills, no individual certification required
- Consultant – Certified CMMC Professional, Registered Practitioner, or no certification required
- Assessor – Certified CMMC Professional, Certified CMMC Assessor individual certifications **are required** to be assessors
- Trainer – Provisional Instructor or Certified CMMC Instructor certifications **are required** to be a trainer that results in training that qualifies students to take the certification exams
- https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles

Key Takeaways

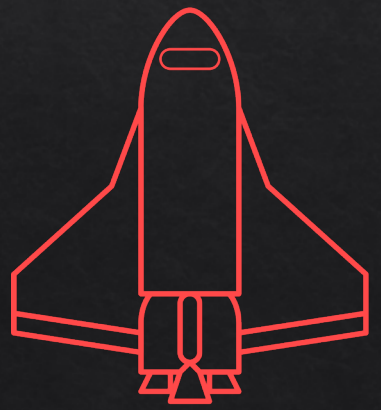
- DoD sponsored CMMC because self-attestation proved ineffective
- CMMC requires third party conformity assessments of NIST SP 800-171
- While the CMMC program still has some ambiguity, the requirements of NIST SP 800-171 are applied to existing contracts with DFARS 7012
- Easy to transition into CMMC from RMF due to commonalities but will require learning a new set of acronyms
- Reading to comprehension is a superpower (GRC also stands for General Reading Comprehension)
- Data protections follow data – limiting data flows can be used to limit assessment scope but you must understand your use cases and authorized data flows

References

- https://csrc.nist.gov/glossary
- https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
- https://dodcio.defense.gov/CMMC/About/
- https://dodcio.defense.gov/Portals/0/Documents/CMMC/Scope_Level2_V2.0_FINAL_20211202_508.pdf
- https://www.cmmcaudit.org/cmmc-2-0-scoping-scenarios-analysis/
- https://cyberab.org/Portals/0/Documents/Process-Documents/CMMC-Assessment-Process-CAP-v1.0.pdf
- https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles

Questions / Contact Information

- Last slide!
- Thanks for listening – now hit me with rabbit hole questions
- Email me: jeff@spacecoastcyber.com
- Engage with me on LinkedIn: https://www.linkedin.com/in/drjeffbaldwin/



Space Coast Cyber