SECURITY REQUIREMENTS FOR DOD FUNDED PROJECTS

MARCH 2024

USC University of Southern California

AGENDA

01 CMMC Overview

02 Plan and Next Steps

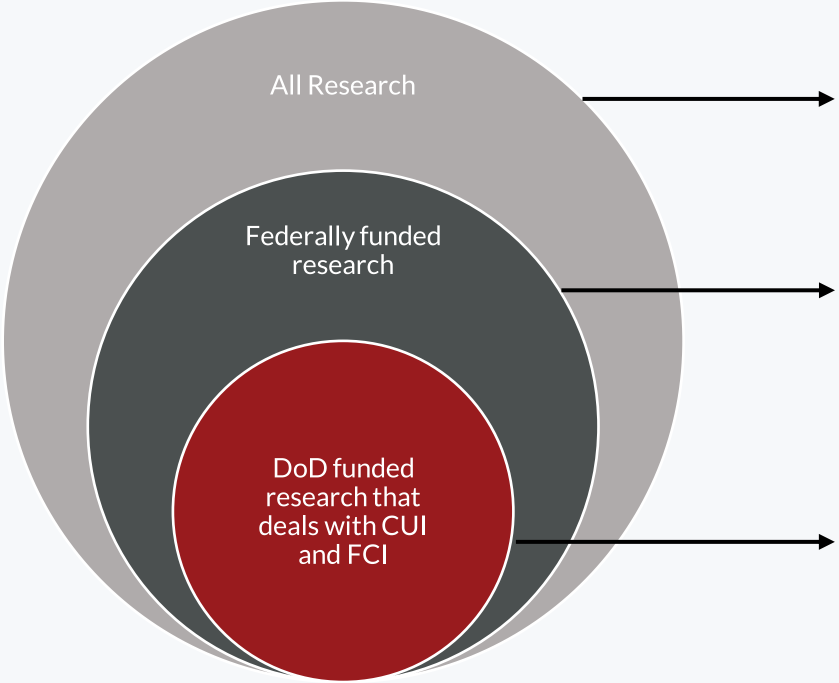
03 Q&A

CMMC OVERVIEW

R
Remember that you are responsible for your actions and how they may affect other fans and athletes, as well as the University.

UNDERSTANDING RESEARCH INFORMATION SECURITY COMPLIANCE AT USC

Research at USC is subject to different types of data security requirements


All Research
Federally funded research
DoD funded research that deals with CUI and FCI

Could be subject to HIPAA, PII

Could be subject to DoD, NIH, NASA and NSF

Focus area that will be subject to DoD cybersecurity mandates (CMMC)

OVERVIEW

Cybersecurity Maturity Model Certification (CMMC) is a security assessment framework that is being mandated by the Department of Defense (DoD) to protect **Controlled Unclassified Information (CUI) and Federal Contracting Information (FCI)** from frequent and increasingly complex cybersecurity risks/obligations. It is intended to safeguard sensitive national security information.

Our goal is to **protect existing research data** and provide the tools and knowledge to **continue to meet requirements** for obtaining DoD research grants

CMMC MODEL

The CMMC level an organization must meet influences compliance and assessment requirements. Applicable levels are determined by the sensitivity of data involved in a research project and will be specified in contracting documents.

CMMC Level	Applicability	Example Data Types	Assessment Requirement	Number of requirements*
1	Handles Federal Contracting Information (FCI)	Information not intended for public release, that is provided by or generated for the Government; Applicable to federally funded research	Self Assessment	17 Controls
2	Handles Controlled Unclassified Information (CUI)	Identified data related to: • National Security Considerations • Export Controls • Geodetic/Terrain Data • Armed Forces Personnel Data • Defense Industrial Design Data • Armed Forces Training Programs & Simulations	Third Party Assessment	110 Controls
3	Handles CUI for DoD Programs impacting National Security	CUI in DoD programs that are considered the greatest risks and potentially impacting Infrastructure and National Security	DoD Assessments with aid of Third Parties	134 Controls

https://www.archives.gov/cui/registry/category-list

*Requirements come from NIST 800-171 revision 2 and 800-172 (applicable for level 3)

FEDERAL CONTRACTING INFORMATION (FCI)

CMMC Level	Definition
1	Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Examples

- Information *from* the Government that is not publicly available
- Emails sent from the Federal Government containing FCI
- Information generated *for* the Government that is not publicly available

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

NARA CUI Categories

Microsoft Excel Worksheet

CMMC Level	Definition
2	Controlled Unclassified Information (CUI) is information that requires controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified. All CUI categories and definitions are published by the National Archives.

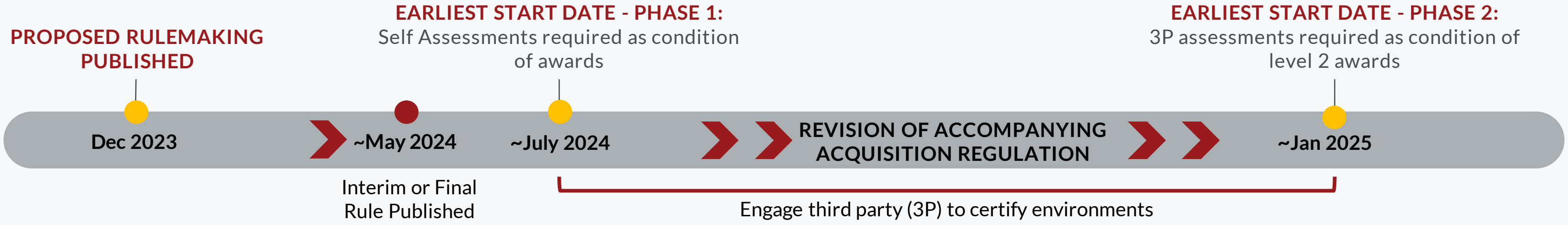
All CUI data as defined by the National Archives must meet level 2 requirements.

Examples

- Defense Controlled Technical Information
- Export Controls
- Geodetic/Terrain Data
- Armed Forces Personnel Data
- Defense Industrial Design Data
- Armed Forces Training Programs & Simulations

TIMELINE AND IMPACT ON USC

Based on a conservative understanding of current timelines*, USC will need a CMMC compliant environment by July 2024 to be awarded additional DoD research awards.



PROPOSED RULEMAKING PUBLISHED

Dec 2023

~May 2024

Interim or Final Rule Published

EARLIEST START DATE - PHASE 1:
Self Assessments required as condition of awards

~July 2024

REVISION OF ACCOMPANYING ACQUISITION REGULATION

Engage third party (3P) to certify environments

EARLIEST START DATE - PHASE 2:
3P assessments required as condition of level 2 awards

~Jan 2025

Considerations:

- Once CMMC goes into effect, requirements will be implemented via a phased approach through 2026
- Unless a waiver is provided by the DoD, failure to meet this timeline may result in risks to funding eligibility
- The phased rollout of CMMC does not negate the need for USC to maintain compliance with existing security requirements in our current awards

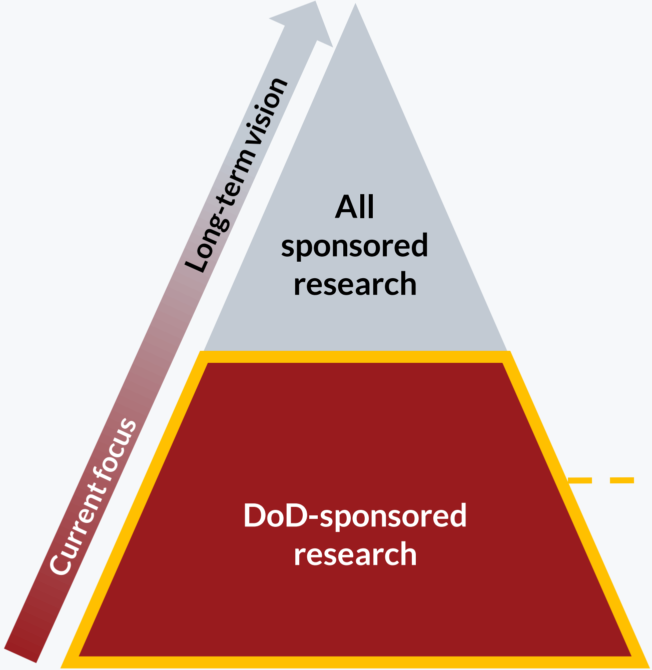
*Timeline based on DoD proposed CMMC rules.

PLAN AND NEXT STEPS

R
Remember that you are responsible for your actions and how they may affect other fans and athletes, as well as the University.

RESEARCH CYBERSECURITY PLAN

The CMMC assessment framework is focused on DoD sponsored research. However, there are other security frameworks that extend beyond just DoD-sponsored research.



CMMC Impacts

DoD-sponsored research projects and supporting functions

1. Self-Assessment (Level 1 and Level 2)

Both Level 1 and Level 2 projects require a self-assessment.

2. Third-Party Assessment (Level 2 only)

Level 2 projects require an additional third-party assessment.

** The current milestone dates are **estimated** based on the anticipated CMMC rule finalization from the Department of Defense.*

WHAT DOES THIS MEAN FOR ME

Impacted projects may be subject to CMMC as early as July, pending the final rule publication.

Impacted Schools*

School	L1	L2
Sol Price		✓
Dornsife	✓	
KSOM	✓	
ICT	✓	✓
ISI	✓	✓
Viterbi	✓	✓

Impacts

Once the CMMC final rule is published (est. May 2024):

- Level 1 assessment requirements may begin to appear in solicitations as early as July 2024
- Third-party assessments may be required as a condition of Level 2 awards as early as January 2025

Unless a waiver is provided by the DoD, failure to meet requirements may result in risks to funding eligibility

* *The full list of schools and projects is subject to change per ongoing validations. List excludes schools with projects ending prior to July 2024.*

COMPLIANCE STRATEGY OVERVIEW

To meet compliance obligations, our strategy must account for the activities that we need to do today and optimize for long term sustainability.

Governance

Requirements

	Short-Term	Long-Term
Level 2	• Establish specific environments for Schools/Units performing the majority of DoD research (ISI, ICT) • Establish central Secure Enclave as-a-service for usage by other schools • Engage common partner to reduce costs	Consolidate service providers to enable a wide range of unique research award IT needs and support Dr. Folt's moonshot while facilitating compliance
Level 1	Build compliance in place at all School/Units where DoD research is performed	• Adjust to meet known future federally funded research security requirements (NSPM-33) • Add additional service providers to enable wide range of unique research award IT needs and support Dr. Folt's moonshot

Timescale

L1 AND L2 TECHNICAL CONTROLS FAMILIES

L1 and L2 CMMC controls have been grouped into 14 high-level families.

🟥 Access Controls	⬛ Audit and Accountability	⬛ Configuration Management	🟥 Identification and Authentication	⬛ Incident Response
⬛ Maintenance	🟥 Media Protection	⬛ Personnel Security	🟥 Physical Protection	⬛ Awareness and Training
⬛ Risk Assessment	🟥 System and Communication Protection	🟥 System and Information Integrity	⬛ Security Assessment	

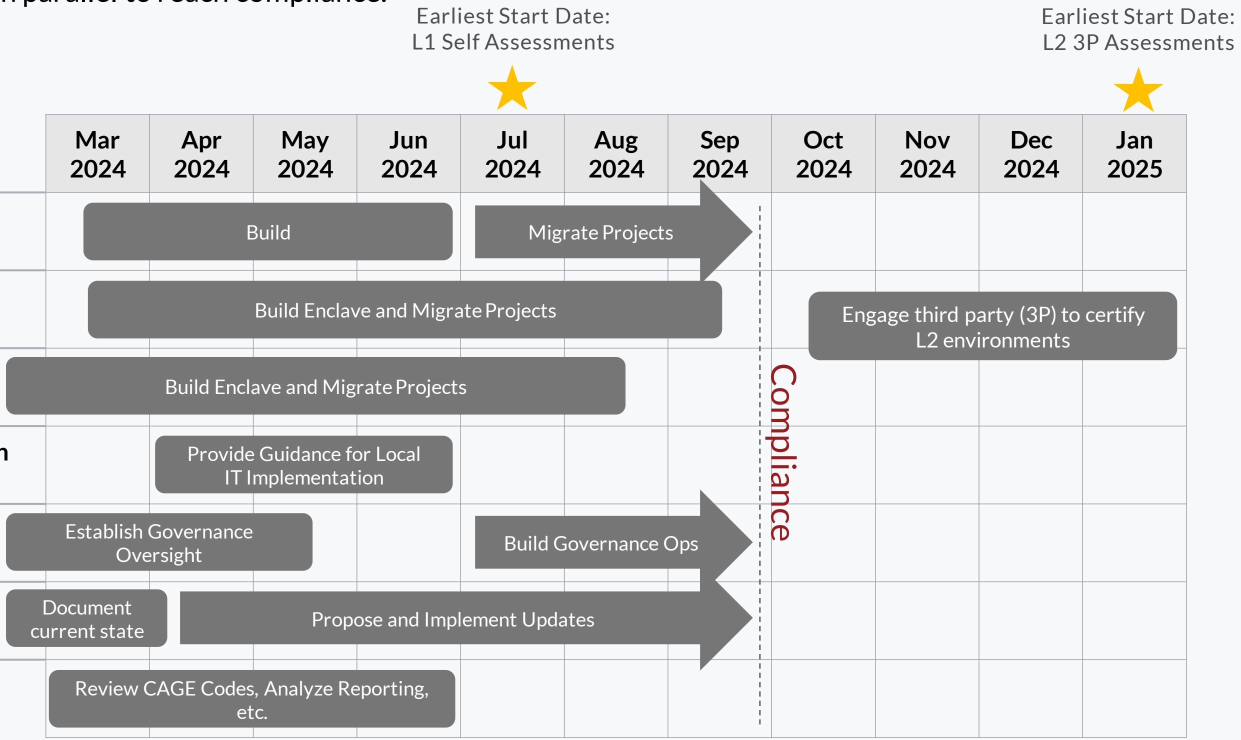
Key

🟥 Both L1 and L2

⬛ L2

CMMC ACTIVITY TIMELINE

Multiple activities need to happen in parallel to reach compliance.



Activity	Mar 2024	Apr 2024	May 2024	Jun 2024	Jul 2024	Aug 2024	Sep 2024	Oct 2024	Nov 2024	Dec 2024	Jan 2025
Level 2: Build Central Enclave	Build				Migrate Projects						
Level 2: ISI Enclave	Build Enclave and Migrate Projects							Engage third party (3P) to certify L2 environments			
Level 2: ICT Enclave	Build Enclave and Migrate Projects										
Level 1: Operationalize Compliance in Place Strategy		Provide Guidance for Local IT Implementation									
Governance Stand-Up	Establish Governance Oversight				Build Governance Ops						
Administrative Controls	Document current state	Propose and Implement Updates									
Logistics Mitigations	Review CAGE Codes, Analyze Reporting, etc.										

OUR ASK OF YOU

Be prepared to identify specific elements within your projects.

ADDITIONAL LEARNING

Attend future information sessions related to the Secure Enclave.
Watch for more information soon.

LEARN WHAT IS IN SCOPE

Learn what projects are in scope by contacting OCEC (Emily Pender).

ADDITIONAL INFORMATION

Be prepared to hear from the Research Security and Regulation Compliance (RSRC) team & OCEC for additional information.

VALIDATE DATA

Be ready to validate data regarding your research, examples including:

1. What type of data do I interact with?
2. Who do I share my data with? Who shares data with me?
3. How do I transmit my data?
4. Where do I store my data?
5. Who has access to my data?

NEXT STEPS

HELP SUPPORT THE TRANSITION TO OUR FUTURE STATE

- Explore the Research Security and Regulation Compliance SharePoint
- Understand upcoming milestones and how to support CMMC compliance
- Watch for future learning opportunities
- Reach out if you have questions

KEY CONTACTS AND RESOURCES

Research Security and Regulatory Compliance (RSRC) at RSRC@usc.edu

RSRC SharePoint: LINK

Office of Culture, Ethics and Compliance (OCEC) compliance@usc.edu

OCEC site: LINK

Q&A

USC University of Southern California

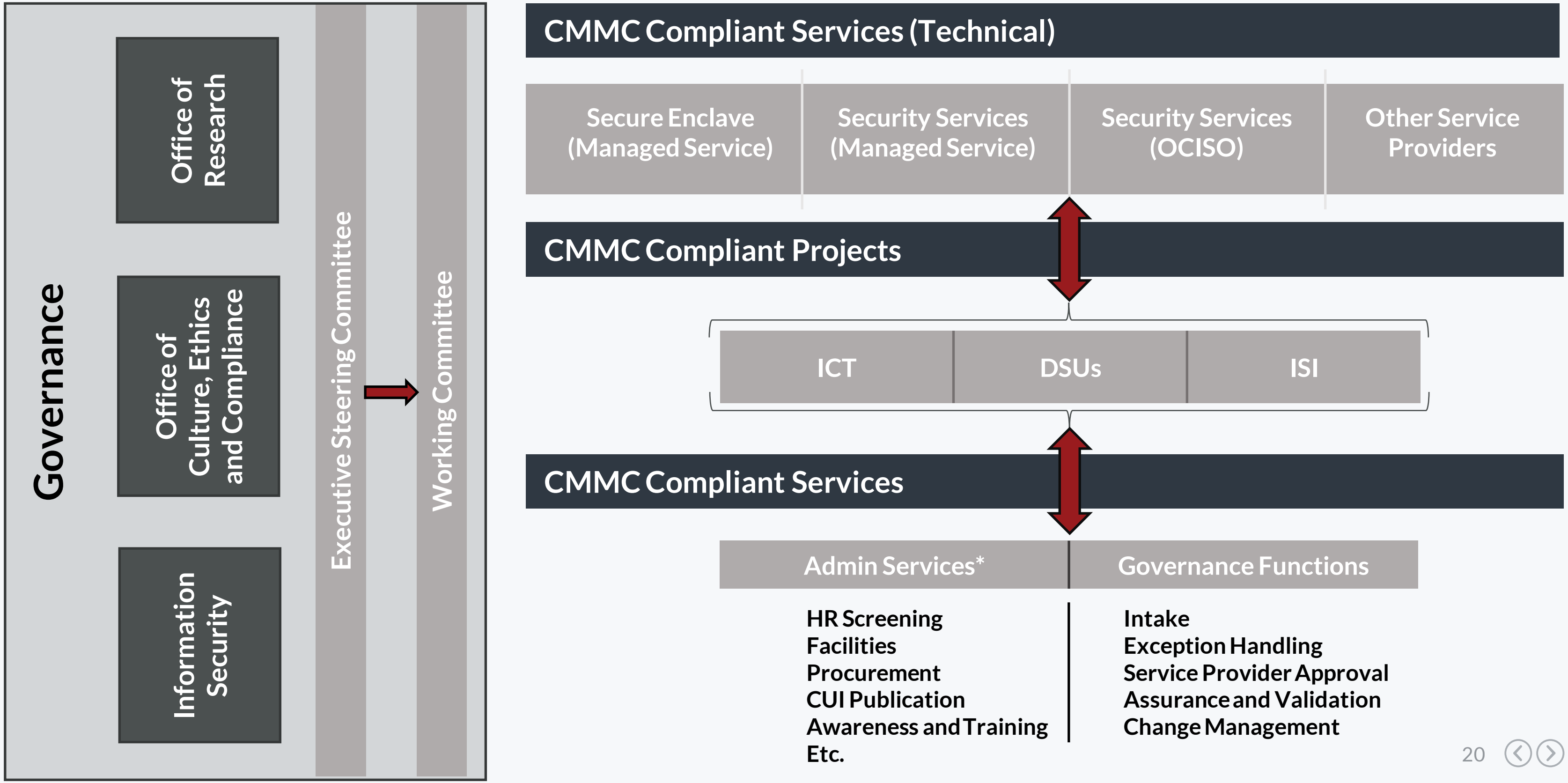
KEY RESOURCES

Use the links below to access the most useful CMMC 2.0 resources.

Resource	Description
About CMMC (defense.gov)	General overview of CMMC including pertinent resources.
CMMC 2.0 Scoping Guidance - Level 1	Guide to leverage when determining the systems in scope for CMMC Level 1.
CMMC 2.0 Scoping Guidance – Level 2	Guide to leverage when determining the systems in scope for CMMC Level 2.
CMMC 2.0 Level 1 Self-Assessment Guide	Guide to leverage to assess CMMC level 1 controls.
CMMC 2.0 Level 2 Assessment Guide	Guide assessors will leverage to assess CMMC level 2 controls.
NIST 800-171 Rev. 2 Control Set	Security controls included in CMMC levels 1-2.
NIST 800-172 Control Set	Security controls to be included in CMMC level 3.
CUI Categories	Official list of CUI categories. Used to help determine when information may be considered CUI.
Federal Register :: Cybersecurity Maturity Model Certification (CMMC) Program	A review of the December 26, 2023 proposed CMMC 2.0 rules

USC University of Southern California

COMPLIANCE VIEW ACROSS THE UNIVERSITY



Governance

Office of Research

Office of Culture, Ethics and Compliance

Information Security

Executive Steering Committee

Working Committee

CMMC Compliant Services (Technical)

Secure Enclave (Managed Service)

Security Services (Managed Service)

Security Services (OCISO)

Other Service Providers

CMMC Compliant Projects

ICT

DSUs

ISI

CMMC Compliant Services

Admin Services*	Governance Functions
HR Screening Facilities Procurement CUI Publication Awareness and Training Etc.	Intake Exception Handling Service Provider Approval Assurance and Validation Change Management

**Only applies to specific processes related to DoD-funded research*

RESEARCH SECURITY COMPLIANCE - TECHNICAL SERVICES

Service Family	Service
Access Control	Data Flow Governance
	Access Request/ Approval/ Implementation/ Removal and Roles
	Privileged Access Management and Role-Based Access Control (PAM + RBAC)
	Endpoint Management/Session Management
	Remote Access
	MDM/BYOD (ties to remote access and device registration)
	User Management (differs from access management as this is authorization as opposed to authentication) and project authorization
	Instance Governance
Audit and Accountability Systems and Information Integrity	Logging and monitoring
	Security Operations Center (SOC), Security Information and Event Management (SIEM), Cyber Threat Intelligence (CTI)
Configuration Management	Device registration/asset management
	Baseline Configuration (Endpoint Configuration Management - ECM)
	Change management (including release management)
Identification and Authentication	MFA
	Password Management
	Privileged Access Mgmt and Role-Based Access Control (PAM + RBAC)
Incident Response	Incident Response Planning
Maintenance	Help Desk and Desktop Support
	Endpoint Management/Session Management

Service Family	Service
Media Protection	Media Tagging (CUI Marking)
	Data Disposition/Destruction
	Removable Media Practices
	Data Flow Governance
	Endpoint Management/Session Management
	Printing Management (to protect from CUI) *only level 2 requirement*
	MDM/BYOD (ties to remote access and device registration)
	Portable Storage Device Policy and Management
Personnel Security	User Management (differs from access management as this is authorization as opposed to authentication) and project authorization
Physical Protection	Known travel (Device Registration/ Physical Protection)
Risk Assessment	Vulnerability Management
	Risk Assessment
System & Communication Protection	SDLC
	Endpoint Management/Session Management
	Key Management Service
System and Information Integrity	Vendor Management and Software Hub
	Logging and monitoring
	Security Operations Center (SOC), Security Information and Event Management (SIEM), Cyber Threat Intelligence (CTI)
System and Communications Protection	Strategic Sourcing