Exploring the Differences between FedRAMP Moderate Certification FedRAMP Moderate Equivalency

In the context of the Federal Risk and Authorization Management Program (FedRAMP), both "FedRAMP Moderate Certified" and "FedRAMP Moderate Equivalency" refer to security compliance levels for cloud service providers (CSPs) who offer services to U.S. federal agencies. However, there are distinctions between the two:

FedRAMP Moderate Certified: This indicates that a cloud service provider has undergone the full FedRAMP authorization process and has been officially certified as meeting the FedRAMP Moderate security baseline. This process involves rigorous assessment, documentation, and testing of the CSP's systems, processes, and security controls to ensure they meet the standards set by FedRAMP.

FedRAMP certification is issued by the ***Joint Authorization Board (JAB)***. The JAB is a key component of the Federal Risk and Authorization Management Program (FedRAMP) responsible for providing provisional authorizations to cloud service providers (CSPs). These provisional authorizations are issued based on the JAB's assessment of a CSP's security posture and compliance with the FedRAMP security requirements.

Cloud service providers seeking FedRAMP certification can undergo a JAB authorization process in addition to or instead of pursuing agency-specific authorizations. The JAB consists of representatives from the Department of Defense (DoD), the Department of Homeland Security (DHS), and the General Services Administration (GSA).

Once a CSP receives a provisional authorization from the JAB, federal agencies can leverage that authorization to use the CSP's cloud services without having to conduct their own separate security assessments. However, it is important to note that the JAB's provisional authorization does not automatically grant full FedRAMP certification. CSPs must still undergo additional steps, including continuous monitoring and reporting, to achieve full FedRAMP certification.

FedRAMP Moderate Equivalency: This term refers to an alternative path for federal agencies to adopt cloud services that have not undergone the formal FedRAMP certification process but can demonstrate an equivalent level of security controls and compliance. This can be achieved through an agency-specific risk assessment (SAR) or through other means that demonstrate compliance with the FedRAMP Moderate baseline. Essentially, it means that while the CSP may not have the official FedRAMP certification, their security measures are deemed equivalent to those required for FedRAMP Moderate certification.

The National Institute of Standards and Technology (NIST) oversees the Federal Risk and Authorization Management Program (FedRAMP). When it comes to issuing a FedRAMP moderate equivalency, it would typically be managed by the FedRAMP Program Management Office (PMO) within NIST. This equivalency may be granted under certain circumstances where a cloud service provider (CSP) has undergone a security assessment and meets security requirements that are equivalent to the FedRAMP moderate baseline,

The role of a ***Third-Party Assessment Organization (3PAO)*** is to conduct security assessments on behalf of cloud service providers (CSPs) seeking FedRAMP certification. Once the assessment is completed, the 3PAO submits their findings and recommendations to the FedRAMP Program Management Office (PMO). The PMO then reviews the assessment report and makes the final determination regarding the CSP's compliance with FedRAMP standards.

In the context of the Cybersecurity Maturity Model Certification (CMMC), achieving FedRAMP Moderate equivalency is a significant requirement for Cloud Service Offerings (CSOs) handling sensitive information for the Department of Defense (DoD). To be considered FedRAMP Moderate equivalent, CSOs must achieve **100 percent compliance with the latest FedRAMP moderate security control baseline, (currently 325 controls)** and maintain a continuous monitoring program to assure compliance with FedRAMP security standards.

In summary, "FedRAMP Moderate Certified" indicates formal certification through the FedRAMP program, while "FedRAMP Moderate Equivalency" suggests that a cloud service provider's security measures are considered equivalent to the FedRAMP Moderate standards, even if they have not undergone the full certification process. It should be noted that Federal Information Systems must use a FedRAMP Moderate Certified CSP. Contractors that support DOD contracts can use a FedRAMP Moderate Equivalency CSP.

FedRAMP Moderate Certification (DOD)

- **FedRAMP Moderate Authorization**: This certification process involves a cloud service provider (CSP) undergoing a rigorous assessment to meet specific security standards. It requires adherence to a defined set of 325 security controls based on NIST SP 800-53. Achieving FedRAMP Moderate Authorization signifies that the CSP has implemented security controls and processes that align with the stringent requirements.

FedRAMP Moderate Equivalency (Commercial)

- **FedRAMP Moderate Equivalency**: On the other hand, FedRAMP Moderate Equivalency refers to a certification that is equivalent in rigor to FedRAMP Moderate but does not replace the need for full FedRAMP Moderate authorization for federal government use. To be considered equivalent, CSPs must achieve 100% compliance with the latest FedRAMP moderate security control baseline, adhere to DFARS 7012 cyber incident/response protocols, and undergo assessment by an accredited Third-Party Assessment Organization (3PAO).

The appendix following the report identifies the controls that are required for FedRAMP Moderate vs those existing in CMMC Level 2

- **HOWEVER,** DOD permits the cloud service to forgo implementation of certain baseline controls if the requesting DOD agency can demonstrate that any controls not implemented by the CSP are being implemented by the DOD Host computing environment which is governed by the controls of NIST-800-53 Rev 5.
- Other agencies that wish to use the same CSP must show that their host environment also implements the controls not provided by the CSP to obtain system accreditation.
- **Commercial organizations** that meet the requirements of CMMC level 2 are only implementing a subset of the 325 controls that NIST / DOD requires to handle sensitive information. Because there will be a minimum of 215 controls that commercial organizations are not implementing, CSP implementation of FedRAMP moderate must show that all 325 controls are implemented and working properly.

Difference Between FedRAMP Moderate and FedRAMP Moderate Equivalency. The distinction between FedRAMP Moderate and FedRAMP Moderate Equivalency lies in the level of compliance and certification process for Cloud Service Providers (CSPs) handling sensitive information for the Department of Defense (DoD).

FedRAMP Moderate:

- **Certification Process:** FedRAMP Moderate authorization involves a rigorous assessment process where a CSP undergoes evaluation against specific security controls to receive certification.
- **Compliance Requirement** CSPs must meet the security standards outlined in the FedRAMP Moderate baseline to ensure data protection and cybersecurity measures are in place.
- **Assessment Criteria:** The assessment focuses on verifying that the CSP has implemented the necessary controls from the FedRAMP Moderate baseline to secure sensitive information.

FedRAMP Moderate Equivalency:

- **Compliance Standard:** Achieving FedRAMP Moderate equivalency requires CSPs to demonstrate 100% compliance with the latest FedRAMP Moderate security control.
- **Documentation:** CSPs must provide detailed documentation, including a System Security Plan, Control Implementation Summary Workbook, Security Assessment Plan, and Security Assessment Report conducted by a Third-Party Assessment Organization (3PAO)
- **Responsibilities Clarification:** Clear delineation of security responsibilities between the CSP and the contractor is essential to meet FedRAMP equivalency standards.

In essence, while FedRAMP Moderate focuses on the certification process and compliance with specific security controls, achieving FedRAMP Moderate Equivalency demands a higher level of compliance with all security controls from the FedRAMP Moderate baseline to ensure robust cybersecurity measures are implemented for handling sensitive information within the DoD framework.

Frequently Asked Questions

Is there is NIST standard for FedRAMP?

Yes, there is a NIST standard that relates to FedRAMP. FedRAMP utilizes the National Institute of Standards and Technology's (NIST) guidelines and procedures to establish standardized security requirements for cloud services. Specifically, FedRAMP leverages NIST's Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations series, including the baselines and test cases. This alignment with NIST standards ensures that cloud service providers seeking FedRAMP authorization must demonstrate compliance with the security controls outlined in NIST 800-53

How does FedRAMP use NIST guidelines and procedures?

FedRAMP utilizes the National Institute of Standards and Technology's (NIST) guidelines and procedures, specifically leveraging NIST's Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations series. This alignment ensures that cloud service providers seeking FedRAMP authorization must demonstrate compliance with the security controls outlined in NIST 800-53. FedRAMP is in the process of revising its materials to align with NIST's updates, including the release of SP 800-53B, Control Baselines for Information Systems and Organizations. Additionally, FedRAMP will update its test cases based on NIST's final version of SP 800-53A - Assessing Security and Privacy Controls in Federal Information Systems and Organizations.

Many controls in NIST 800-53B are not allocated to a baseline - where do they belong?

In NIST Special Publication 800-53B, some controls are not allocated to a baseline. These controls are intended to be customized by organizations based on their specific security and privacy needs. The control baselines provided in SP 800-53B serve as a starting point for organizations in the security and privacy control selection process. By using the tailoring guidance and assumptions provided, organizations can customize these controls to ensure they have the capability to protect their critical operations and assets effectively. This customization allows organizations to address their unique security and privacy requirements.

Can a cloud service provider achieve FedRAMP certification with POA&M items?

A Cloud Service Provider (CSP) pursuing FedRAMP certification cannot address gaps within a Plan of Action and Milestones (POA&M). FedRAMP Ready designation indicates a CSP's readiness for authorization, but gaps must be addressed before achieving full authorization. To achieve FedRAMP compliance, a CSP must conduct an assessment, receive authorization, and maintain continuous monitoring of their cybersecurity measures. FedRAMP compliance is essential for any CSP working with federal agencies, ensuring adherence to strict security standards and authorization processes.

To achieve FedRAMP certification, Cloud Service Providers (CSPs) must follow a structured process that involves several key steps. Here is an overview of the process for achieving FedRAMP certification:

Steps to Achieve FedRAMP Certification:

1. **Preparation Phase**:
    - Select an authorization approach: either through the Joint Authorization Board (JAB) or a federal agency.
    - Complete Partnership Establishment and Readiness Assessment.
2. **Authorization Phase**:
    - Conduct a Full Security Assessment with deliverables like SSP, SAP, SAR, and POA&M.
    - Undergo an agency review of the security authorization package.
    - Address any findings from the Security Assessment Report (SAR) issued by the 3PAO.
    - Obtain Provisional Authorization to Operate (P-ATO) from JAB or an Agency Authorization.
3. **Continuous Monitoring**:
    - Engage in continuous monitoring to ensure ongoing compliance with FedRAMP standards.

The timeline for the FedRAMP process typically involves four phases: System Development and Preparation, Agency Sponsorship, Security Assessment lasting 7-10 weeks, and Continuous Monitoring. The process can be complex and time-consuming, requiring collaboration across the organization and adherence to strict security controls Continuous monitoring is crucial post-authorization to maintain compliance with federal security standards. By following these steps diligently and meeting all requirements, CSPs can achieve FedRAMP certification, enabling them to work with federal agencies securely and efficiently.

Can a 3PAO issue a FedRAMP certification?

No, a Third-Party Assessment Organization (3PAO) cannot issue a FedRAMP certification directly. The role of a 3PAO is to conduct security assessments on behalf of cloud service providers (CSPs) seeking FedRAMP certification. These assessments involve evaluating the CSP's systems, processes, and security controls to ensure compliance with the FedRAMP security requirements.

Once the assessment is completed, the 3PAO submits their findings and recommendations to the FedRAMP Program Management Office (PMO). The PMO then reviews the assessment report and makes the final determination regarding the CSP's compliance with FedRAMP standards. If the PMO determines that the CSP meets all the necessary requirements, they issue the FedRAMP authorization, which certifies the CSP's cloud services for use by federal agencies.

In summary, while 3PAOs play a crucial role in the FedRAMP certification process by conducting security assessments, they do not have the authority to issue certifications themselves. The final certification decision rests with the FedRAMP PMO.

Can the Joint authorization board (JAB) issue a FedRAMP certification?

Yes, the Joint Authorization Board (JAB) can issue a FedRAMP certification. The JAB is a key component of the Federal Risk and Authorization Management Program (FedRAMP) responsible for providing provisional authorizations to cloud service providers (CSPs). These provisional authorizations are issued based on the JAB's assessment of a CSP's security posture and compliance with the FedRAMP security requirements.

Cloud service providers seeking FedRAMP certification can undergo a JAB authorization process in addition to or instead of pursuing agency-specific authorizations. The JAB consists of representatives from the Department of Defense (DoD), the Department of Homeland Security (DHS), and the General Services Administration (GSA).

Once a CSP receives a provisional authorization from the JAB, federal agencies can leverage that authorization to use the CSP's cloud services without having to conduct their own separate security assessments. However, it is important to note that the JAB's provisional authorization does not automatically grant full FedRAMP certification. CSPs must still undergo additional steps, including continuous monitoring and reporting, to achieve full FedRAMP certification.

Steven Senz is the CEO of ASCERTIS Solutions. He was a key advisor to the federal government for cyber-security and cloud migration. He has presented to multiple Federal and Commercial forums on cyber security issues dealing with privacy and e-mail fraud. From 2006, Steve consulted to the intelligence community and participated in multiple working groups as the community migrated to an environment where information sharing between agencies was considered essential for situational awareness. Steven has assisted numerous ISSMs in accrediting federal information systems and environments, to assure that classified information is properly protected and transmitted in digital and hardcopy forms. Steven holds a Master's degree from Cornell University and the University of Michigan, as well as numerous security certifications from (ISC)2, ISACA and George Washington University

ASCERTIS Solutions is based in Virginia. We provide the most cost effective commercial CMMC assessment tool on the market. We also provide assistance in developing company Policies and Procedures that are compliant with CMMC/DOD requirements. If your organization is seeking to become CMCC certified at either Level 1 or Level – please log onto HTTPS://Ascertis.solutions.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

CMMC Level 2 Controls					
ID	FAMILY	# Controls	ID	FAMILY	# Controls
AC	Access Control	22	MP	Media Protection	9
AT	Awareness and Training	3	PS	Personnel Security	2
AU	Audit and Accountability	9	PE	Physical Protection	6
CM	Configuration Management	9	RA	Risk Assessment	3
IA	Identification and Authentication	11	CA	Security Assessment	4
IR	Incident Response	3	SC	System and Communications Protection	16
MA	Maintenance	6	SI	System and Information Integrity	7

Total Controls = 110

FedRAMP Moderate Baseline Controls					
ID	FAMILY	# Controls	ID	FAMILY	# Controls
AC	Access Control	39	PE	Physical and Environmental Protection	18
AT	Awareness and Training	6	PL	Planning	7
AU	Audit and Accountability	16	PM	Program Management	32
CA	Assessment, Authorization, and Monitoring	10	PS	Personnel Security	9
CM	Configuration Management	24	PT	PII Processing and Transparency	8
CP	Contingency Planning	22	RA	Risk Assessment	10
IA	Identification and Authentication	24	SA	System and Services Acquisition	16
IR	Incident Response	13	SC	System and Communications Protection	25
MA	Maintenance	9	SI	System and Information Integrity	18
MP	Media Protection	7	SR	Supply Chain	12

Total Controls = 325

Control families in Red have been added in NIST 800-53 Rev 5

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Access Control	AC-1	Policies & Procedures	1	**Access Control**			
	AC-2	Account Mngt	7		AC.L1-3.1.1	Account Mngt	1
	AC-3	Access Enforcement	1		AC.L1-3.1.2	Access Enforcement	1
	AC-4	Inform Flow Enforcement	1		AC.L2-3.1.3	Inform Flow Enforcement	1
	AC-5	Separate of Duties	1		AC.L2-3.1.4	Separate of Duties	1
	AC-6	Least Privilege	7		AC.L2-3.1.5, 6, 7	Least Privilege	3
	AC-7	Unsuccessful Login Attempts	1		AC.L2-3.1.8	Unsuccessful Login Attempts	1
	AC-8	System Use notification	1		AC.L2-3.1.9	System Use notification	1
	AC-9	Previous logon Notification	0				
	AC-10	Concurrent Session Control	0				
	AC-11	Device lock	1		AC.L2-3.1.10	Session Lock	1
	AC-12	Session Termination	2		AC.L2-3.1.11	Session Termination	1
	AC-13	Supervision & Review (deleted)	0				
	AC-14	Guest Login	1				
	AC-15	Automated Marking (deleted)	0				
	AC-16	Security & Privacy Attributes	0				
	AC-17	Remote Access	5		AC.L2-3.1.12, 13, 14, 15	Remote Access	4
	AC-18	Wireless Access	3		AC.L2-3.1.16, 17	Wireless Access	2
	AC-19	Mobile Device Access control	2		AC.L2-3.1.18, 19	Mobile Device Access control	2
	AC-20	Use of External Systems	3		AC.L1-3.1.20, AC.L2.1.21	User of External Systems	2
	AC-21	Information Sharing	1				
	AC-22	Publicly Accessible Content	1		AC.L1-3.1.22	Publicly Accessible Content	1
	AC-23	Data Mining Protection	0				
	AC-24	Access Control Decision	0				
	AC-25	Reference Monitor	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Awareness & Training	AT-1	Policies & Procedures	1	**Awareness & Training**	AT.L2-3.2.1	Awareness Training	1
	AT-2	Literacy Training & Awareness	3		AT.L2-3.2.3	Awareness Training	1
	AT-3	Role Based Training	1		AT.L2-3.2.2	Role Based Training	1
	AT-4	Training Records	1				
	AT-5	Security Group Contacts (deleted)	0				
	AT-6	Training feedback	0				

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Audit & Accountability	AU-1	Policy and Procedures	1	**Audit & Accountability**			
	AU-2	Event Logging	1		AU.L2-3.3.1	Audit Events	1
	AU-3	Content of Audit Records	2		AU.L2-3.3.2	Basic Audit Information	1
	AU-4	Audit Log Storage Capacity	1				
	AU-5	Response to Audit Logging Process Failures	1		AU.L2-3.3.4	Response to Audit Logging Process Failures	1
	AU-6	Audit Record Review, Analysis, and Reporting	3		AU.L2-3.3.3, 5	Audit Record Review, Analysis, and Reporting	2
	AU-7	Audit Record Reduction and Report Generation	2		AU.L2-3.3.6	Audit Record Reduction and Report Generation	1
	AU-8	Time Stamps	1		AU.L2-3.3.7	Time Stamps	1
	AU-9	Protection of Audit Information	2		AU.L2-3.3.8, 9	Protection of Audit Information	2
	AU-10	Non-repudiation	0				
	AU-11	Audit Record Retention	1				
	AU-12	Audit Record Generation	1				
	AU-13	Monitoring for Information Disclosure	0				
	AU-14	Session Audit	0				
	AU-15	Alternate Audit Logging Capability	0				
	AU-16	Cross-Organizational Audit Logging	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Assessment, Authorization and Monitoring	CA-1	Policy and Procedures	1	**Security Assessment**			
	CA-2	Control Assessments	2		CA.L2-3.12.1	Security Assessment	1
	CA-3	Information Exchange	1				
	CA-4	Security Certification (deleted)	0				
	CA-5	Plan of Action and Milestones	1		CA.L2-3.12.2	Plan of Action and Milestones	1
	CA-6	Authorization	1				
	CA-7	Continuous Monitoring	3		CA.L2-3.12.3	Continuous Monitoring	1
	CA-8	Penetration Testing	0				
	CA-9	Internal System Connections	1				
					CA.L2-3.12.4	System Security Plan	1

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Configuration Management	CM-1	Policy and Procedures	1	**Configuration Management**			
	CM-2	Baseline Configuration	4		CM.L2.3.4.1	Baseline Configuration	1
	CM-3	Configuration Change Control	3		CM.L2.3.4.3	Configuration Change Control	1
	CM-4	Impact Analyses	2		CM.L2.3.4.4	Impact Analyses	1
	CM-5	Access Restrictions for Change	1		CM.L2.3.4.5	Access Restrictions for Change	1
	CM-6	Configuration Settings	1		CM.L2.3.4.2	Configuration Settings	1
	CM-7	Least Functionality	4		CM.L2.3.4.6, 7, 8	Least Functionality	3
	CM-8	System Component Inventory	3				
	CM-9	Configuration Management Plan	1				
	CM-10	Software Usage Restrictions	1				
	CM-11	User-Installed Software	1		CM.L2.3.4.9	User-Installed Software	1
	CM-12	Information Location	2				
	CM-13	Data Action Mapping	0				
	CM-14	Signed Components	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Contingency Planning	CP-1	Policy and Procedures	1	**Contingency Planning**			
	CP-2	Contingency Plan	3				
	CP-3	Contingency Training	1				
	CP-4	Contingency Plan Testing	2				
	CP-5	Contingency Plan Update (deleted)	0				
	CP-6	Alternate Storage Site	3				
	CP-7	Alternate Processing Site	4				
	CP-8	Telecommunications Services	3				
	CP-9	System Backup	3				
	CP-10	System Recovery and Reconstitution	2				
	CP-11	Alternate Communications Protocols	0				
	CP-12	Safe Mode	0				
	CP-13	Alternative Security Mechanisms	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Identification & Authentication	IA-1	Policy and Procedures	1	**Identification & Authentication**			
	IA-2	Identification and Authentication (Organizational Users)	5		IA.L1-3.5.1, IA/L2-3.5.3, 4	Identification and Authentication (Organizational Users)	3
	IA-3	Device Identification and Authentication	1		IA.L1-3.5.2	Device Identification and Authentication	1
	IA-4	Identifier Management	2		IA.L2-3.5.5, 6	Identifier Management	2
	IA-5	Authenticator Management	4		IA.L2-3.5.7, 8, 9, 10	Authenticator Management	4
	IA-6	Authentication Feedback	1		IA.L2-3.5.11	Authentication Feedback	1
	IA-7	Cryptographic Module Authentication	1				
	IA-8	Identification and Authentication (Non-Organizational Users)	4				
	IA-9	Service Identification and Authentication	0				
	IA-10	Adaptive Authentication	0				
	IA-11	Re-authentication	1				
	IA-12	Identity Proofing	4				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

FedRAMP Moderate Control Baseline				CMMC Level 2			
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Incident Response	IR-1	Policy and Procedures	1	**Incident Response**			
	IR-2	Incident Response Training	1		IR.L2-3.6.1	Incident Response Training	1
	IR-3	Incident Response Testing	2		IR.L2-3.6.3	Incident Response Testing	1
	IR-4	Incident Handling	2		IR.L1-3.6.2	Incident Handling	1
	IR-5	Incident Monitoring	1				
	IR-6	Incident Reporting	3				
	IR-7	Incident Response Assistance	2				
	IR-8	Incident Response Plan	1				
	IR-10	Integrated Information Security Analysis Team (deleted)	0				

FedRAMP Moderate Control Baseline				CMMC Level 2			
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Maintenance	MA-1	Policy and Procedures	1	**Maintenance**			
	MA-2	Controlled Maintenance	1		MA.L2-3.7.1, 3	Controlled Maintenance	2
	MA-3	Maintenance Tools	4		MA.L2-3.7.2, 4	Maintenance Tools	2
	MA-4	Nonlocal Maintenance	1		MA.L2-3.7.5	Nonlocal Maintenance	1
	MA-5	Maintenance Personnel	1		MA.L2-3.7.6	Maintenance Personnel	1
	MA-6	Timely Maintenance	1				
	MA-7	Field Maintenance	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Media Protection	MP-1	Policy and Procedures	1	**Media Protection**			
	MP-2	Media Access	1		MP.2-3.8.1	Media Access	1
	MP-3	Media Marking	1		MP.2-3.8.4	Media Marking	1
	MP-4	Media Storage	1		MP.2-3.8.2	Media Storage	1
	MP-5	Media Transport	1		MP.2-3.8.5, 6	Media Transport	2
	MP-6	Media Sanitization	1		MP.L1-3.8.3	Media Sanitization	1
	MP-7	Media Use	1		MP.L2-3.8.7, 8	Media Use	2
	MP-8	Media Downgrading	0				
					MP.L2-3.8.0	Information System Backup	1

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

FedRAMP Moderate Control Baseline					CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Physical and Environmental Protection	PE-1	Policy and Procedures	1	**Physical Protection**			
	PE-2	Physical Access Authorizations	1		PE.L1-3.10.1	Physical Access Authorizations	1
	PE-3	Physical Access Control	1		PE.L1-3.10.3, 4, 5	Physical Access Control	3
	PE-4	Access Control for Transmission	1				
	PE-5	Access Control for Output Devices	1				
	PE-6	Monitoring Physical Access	2		PE.L2-3.10.2	Monitoring Physical Access	1
	PE-7	Visitor Control (deleted)	0				
	PE-8	Visitor Access Records	1				
	PE-9	Power Equipment and Cabling	1				
	PE-10	Emergency Shutoff	1				
	PE-11	Emergency Power	1				
	PE-12	Emergency Lighting	1				
	PE-13	Fire Protection	2				
	PE-14	Environmental Controls	1				
	PE-15	Water Damage Protection	1				
	PE-16	Delivery and Removal	1				
	PE-17	Alternate Work Site	1		PE.L2-3.10.6	Alternate Work Site	1
	PE-18	Location of System Components	0				
	PE-19	Information Leakage	0				
	PE-20	Asset Monitoring and Tracking	0				
	PE-21	Electromagnetic Pulse Protection	0				
	PE-22	Component Marking	0				
	PE-23	Facility Location	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Planning	PL-1	Policy and Procedures	1	**Security Assessment**			
	PL-2	System Security and Privacy Plans	1		CA L2-3.12-4	System Security Plans	1
	PL-4	Rules of Behavior	2				
	PL-5	Privacy Impact Assessment (deleted)	0				
	PL-6	Security-Related Activity Planning (de	0				
	PL-7	Concept of Operations					
	PL-8	Security and Privacy Architectures	1				
	PL-9	Central Management	0				
	PL-10	Baseline Selection	1				
	PL-11	Baseline Tailoring	1				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Program Management	PM-1	Information Security Program Plan	Deployed organization-wide. Supports information security program. Not associated with security control baselines. Independent				
	PM-2	Information Security Program Leadership Role					
	PM-3	Information Security and Privacy Resources					
	PM-4	Plan of Action and Milestones Process					
	PM-5	System Inventory					
	PM-6	Measures of Performance					
	PM-7	Enterprise Architecture					
	PM-8	Critical Infrastructure Plan					
	PM-9	Risk Management Strategy					
	PM-10	Authorization Process					
	PM-11	Mission and Business Process Definition					
	PM-12	Insider Threat Program					
	PM-13	Security and Privacy Workforce					
	PM-14	Testing, Training, and Monitoring					
	PM-15	Security and Privacy Groups and Associations					
	PM-16	Threat Awareness Program					
	PM-17	Protecting Controlled Unclassified Information on External Systems					
	PM-18	Privacy Program Plan					
	PM-19	Privacy Program Leadership Role					

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	PM-20	Dissemination of Privacy Program Information	of any system impact level.				
	PM-21	Accounting of Disclosures					
	PM-22	Personally Identifiable Information Quality Management					
	PM-23	Data Governance Body					
	PM-24	Data Integrity Board					
	PM-25	Minimization of Personally Identifiable Information Used in Testing, Training, and Research					
	PM-26	Complaint Management					
	PM-27	Privacy Reporting					
	PM-28	Risk Framing					
	PM-29	Risk Management Program Leadership Roles					
	PM-30	Supply Chain Risk Management					
	PM-31	Continuous Monitoring Strategy					
	PM-32	Purposing					

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Personnel Security	PS-1	Policy and Procedures	1	**Personnel Security**			
	PS-2	Position Risk Designation	1				
	PS-3	Personnel Screening	1		PS.L2-3.9.1	Personnel Screening	1
	PS-4	Personnel Termination	1		PS.L2-3.9.2	Personnel Termination	1
	PS-5	Personnel Transfer	1				
	PS-6	Access Agreements	1				
	PS-7	External Personnel Security	1				
	PS-8	Personnel Sanctions	1				
	PS-9	Position Descriptions	1				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
PII Processing and Transparency	PT-1	Policy and Procedures	Personally Identifiable Information Processing and Transparency controls are not allocated to the security control baselines.				
	PT-2	Authority to Process Personally Identifiable Information					
	PT-3	Personally Identifiable Information Processing Purposes					
	PT-4	Consent					
	PT-5	Privacy Notice					
	PT-6	System of Records Notice					
	PT-7	Specific Categories of Personally Identifiable Information					
	PT-8	Computer Matching Requirements					

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Risk Assessment	RA-1	Policy and Procedures	1	**Risk Assessment**			
	RA-2	Security Categorization	1				
	RA-3	Risk Assessment	2		RA.L2-3.11.1	Risk Assessment	1
	RA-4	Risk Assessment Update (deleted)	0				
	RA-5	Vulnerability Monitoring and Scannir	4		RA.L2-3.11.2, 3	Vulnerability Monitoring and Scannir	2
	RA-6	Technical Surveillance Countermeasures Survey	0				
	RA-7	Risk Response	1				
	RA-8	Privacy Impact Assessments	0				
	RA-9	Criticality Analysis	1				
	RA-10	Threat Hunting	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
System and Services Acquisition	SA-1	Policy and Procedures	1	**Security Assessment**			
	SA-2	Allocation of Resources	2				
	SA-3	System Development Life Cycle	1				
	SA-4	Acquisition Process	5				
	SA-5	System Documentation	1				
	SA-6	Software Usage Restrictions (deleted)	0				
	SA-7	User-Installed Software (deleted)	0				
	SA-8	Security and Privacy Engineering Prin	1		SC.L2-3.13.2	Security and Privacy Engineering Principles	1
	SA-9	External System Services	2				
	SA-10	Developer Configuration Managemer	1				
	SA-11	Developer Testing and Evaluation	1				
	SA-12	Supply Chain Protection (deleted)	0				
	SA-13	Trustworthiness (deleted)	0				
	SA-14	Criticality Analysis (deleted)	0				
	SA-15	Development Process, Standards, an	0				
	SA-16	Developer-Provided Training	0				
	SA-17	Developer Security and Privacy Architecture and Design	0				
	SA-18	Tamper Resistance and Detection (de	0				
	SA-19	Component Authenticity (deleted)	0				
	SA-20	Customized Development of Critical Components	0				
	SA-21	Developer Screening	0				
	SA-22	Unsupported System Components	1				
	SA-23	Specialization					

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
System and Communications Protection	SC-1	Policy and Procedures	1	**System and Communications Protection**			
	SC-2	Separation of System and User Funct	1				
	SC-3	Security Function Isolation	0				
	SC-4	Information in Shared System Resources	1		SC.L2-3.13.4	Information in Shared System Resources	1
	SC-5	Denial-of-Service Protection	1				
	SC-6	Resource Availability					
	SC-7	Boundary Protection	6		SC.L1-3.13.1, 5 SC.L2-3.13.6, 7	Boundary Protection	4
	SC-8	Transmission Confidentiality and Integrity	2		SC.L2-3.13.8	Transmission Confidentiality and Integrity	1
	SC-9	Transmission Confidentiality (deleted)	0				
	SC-10	Network Disconnect	1		SC.L2-3.13.9	Network Disconnect	1
	SC-11	Trusted Path	0				
	SC-12	Cryptographic Key Establishment and Management	1		SC.L2-3.13.10	Cryptographic Key Establishment and Management	1
	SC-13	Cryptographic Protection	1		SC.L2-3.13.11	Cryptographic Protection	1
	SC-14	Public Access Protections (deleted)	0				
	SC-15	Collaborative Computing Devices and Applications	1		SC.L2-3.13.12	Collaborative Computing Devices and Applications	1
	SC-16	Transmission of Security and Privacy Attributes	0				
	SC-17	Public Key Infrastructure Certificates	1				
	SC-18	Mobile Code	1		SC.L2-3.13.13	Mobile Code	1
	SC-19	Voice over Internet Protocol	0		SC.L2-3.13.14	Voice over Internet Protocol	1

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
System and Communications Protection	SC-20	Secure Name/Address Resolution Service (Authoritative Source)	1	**System and Communications Protection**			
	SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	1				
	SC-22	Architecture and Provisioning for Name/Address Resolution Service	1				
	SC-23	Session Authenticity	1		SC.L2-3.13.15	Session Authenticity	1
	SC-24	Fail in Known State	0				
	SC-25	Thin Nodes	0				
	SC-26	Decoys	0				
	SC-27	Platform-Independent Applications	0				
	SC-28	Protection of Information at Rest	1		SC.L2-3.13.16	Protection of Information at Rest	1
	SC-29	Heterogeneity	1				
	SC-30	Concealment and Misdirection	0				
	SC-31	Covert Channel Analysis	0				
	SC-32	System Partitioning	0		SC.L2-3.13.3	Application Partitioning	1
	SC-33	Transmission Preparation Integrity (c	0				
	SC-34	Non-Modifiable Executable Programs	0				
	SC-35	External Malicious Code Identificatio	0				
	SC-36	Distributed Processing and Storage	0				
	SC-37	Out-of-Band Channels	0				
	SC-38	Operations Security	0				
	SC-39	Process Isolation	1				
	SC-40	Wireless Link Protection	0				
	SC-41	Port and I/O Device Access	0				
	SC-42	Sensor Capability and Data	0				
	SC-43	Usage Restrictions	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
System and Communications Protection	SC-44	Detonation Chambers	0	**System and Communications Protection**			
	SC-45	System Time Synchronization	0				
	SC-46	Cross Domain Policy Enforcement	0				
	SC-47	Alternate Communications Paths	0				
	SC-48	Sensor Relocation	0				
	SC-49	Hardware-Enforced Separation and Policy Enforcement	0				
	SC-50	Software-Enforced Separation and Policy Enforcement	0				
	SC-51	Hardware-Based Protection	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
System and Information Integrity	SI-1	Policy and Procedures	1	**System and Information Integrity**			
	SI-2	Flaw Remediation	2		SI.L1-3.14.1, 2	Flaw Remediation	2
	SI-3	Malicious Code Protection	1		SI.L1-3.14.4, 5	Malicious Code Protection	2
	SI-4	System Monitoring	4		SI.L2-3.14.6, 7	System Monitoring	2
	SI-5	Security Alerts, Advisories, and Direct	1		SI.L2-3.14.3	Security Alerts, Advisories, and Directives	1
	SI-6	Security and Privacy Function Verifica	0				
	SI-7	Software, Firmware, and Information	3				
	SI-8	Spam Protection	2				
	SI-9	Information Input Restrictions (delete	0				
	SI-10	Information Input Validation	1				
	SI-11	Error Handling	1				
	SI-12	Information Management and Retent	1				
	SI-13	Predictable Failure Prevention	0				
	SI-14	Non-Persistence	0				
	SI-15	Information Output Filtering	0				
	SI-16	Memory Protection	1				
	SI-17	Fail-Safe Procedures	0				
	SI-18	Personally Identifiable Information Q	0				
	SI-19	De-identification	0				
	SI-20	Tainting	0				
	SI-21	Information Refresh	0				
	SI-22	Information Diversity	0				
	SI-23	Information Fragmentation	0				

Controls in red that are marked “Deleted” have been incorporated into other controls.

Summary of Security Controls between CMMC Level 2 and FedRAMP Moderate

	FedRAMP Moderate Control Baseline				CMMC Level 2		
Control Family	Control Number	Name	With Enhancement	Control Family	Control Number(s)	Name	With Enhancement
Supply Chain	SR-1	Policy and Procedures	1				
	SR-2	Supply Chain Risk Management Plan	2				
	SR-3	Supply Chain Controls and Processe	1				
	SR-4	Provenance	0				
	SR-5	Acquisition Strategies, Tools, and Me	1				
	SR-6	Supplier Assessments and Reviews	1				
	SR-7	Supply Chain Operations Security	0				
	SR-8	Notification Agreements	1				
	SR-9	Tamper Resistance and Detection	0				
	SR-10	Inspection of Systems or Component	1				
	SR-11	Component Authenticity	3				
	SR-12	Component Disposal	1				

Controls in red that are marked “Deleted” have been incorporated into other controls.