imprivata

Checklist: Understanding the requirements of CMMC 2.0 for manufacturers

As of November 2025, manufacturers or supply chain vendors must demonstrate compliance with the **Cybersecurity Maturity Model Certification (CMMC) 2.0** framework before they can be awarded a Department of Defense (DOD) contract. This applies to direct contractors as well as vendors throughout the supply chain.

Simply put: if your organization wants to win or retain DOD business, CMMC 2.0 compliance isn't optional.

Use the following list to align your security measures with CMMC 2.0 [Level 2]. Each control helps reduce risk and improve audit readiness.

Multifactor authentication (MFA)

Strengthening access security: requires users to verify their identity using two or more authentication factors before accessing systems containing controlled unclassified information (CUI)

Why it matters: prevents unauthorized access, phishing attacks, and credential theft

Unique identification and authentication

Eliminating shared accounts: every user must have a unique identifier and authenticate before accessing systems

Why it matters: prevents the use of shared or generic accounts, ensuring accountability and traceability

Password management

Enforcing strong password policies: requires strong, unique passwords and the implementation of password management policies

Why it matters: weak passwords remain a leading cause of breaches and unauthorized access

Account lockout policy

Preventing brute-force attacks: locks a user's account after a certain number of failed login attempts

Why it matters: blocks attackers from using automated brute-force techniques to guess passwords

Privileged account authentication

Securing admin and elevated access: applies additional authentication and controls to privileged accounts

Why it matters: only admin and privileged users should have access to critical systems to prevent attacks

Authentication for remote access

Protecting remote connections: ensures that all remote access is secured with strong authentication measures, such as MFA

Why it matters: remote access is a major attack vector, making secure authentication essential

Device authentication

Ensuring only trusted devices can connect: requires devices to authenticate before connecting to the network

Why it matters: prevents unauthorized or compromised devices from gaining access

Session timeout and reauthentication

Preventing unauthorized access from idle sessions: automatically locks a session or logs a user out after a period of inactivity

Why it matters: prevents unauthorized access if a user leaves a workstation unattended

Cryptographic authentication

Encrypting credentials to prevent interception: uses cryptographic authentication to secure login credentials and prevent unauthorized access

Why it matters: ensures that passwords and authentication tokens are not intercepted or exposed

Enforcement of least privilege and role-based access control

Limiting access based on job role and necessity: ensures users are granted only the minimum level of access required to perform their job functions, based on defined roles and responsibilities.

Why it matters: reduces the risk of insider threats, credential misuse, and lateral movement by restricting access to sensitive systems and controlled unclassified information (CUI) to authorized users only.

Logging and audit of authentication and access events

Capturing and retaining security-relevant events: ensures key activities (such as authentication attempts, access to systems containing controlled unclassified information (CUI), and use of privileged accounts) are logged, reviewed regularly, and retained in accordance with policy.

Why it matters: provides traceability and accountability, supports incident detection and investigation, and enables manufacturers to demonstrate compliance during CMMC assessments by showing who accessed what, when, and how.

Explore Imprivata solutions for manufacturing