✅ CMMC Readiness Checklist for SMBs

Provided by EmTech CyberShield™ Team

🔍 Step 1: Identify Your Data Type

- [ ] Determine if you handle **FCI** (Federal Contract Information)
- [ ] Determine if you handle **CUI** (Controlled Unclassified Information)
- [ ] Confirm your required **CMMC Level** (Level 1 for FCI, Level 2 for CUI)

🧩 Step 2: Scope Your Environment

- [ ] Identify systems that store, process, or transmit FCI/CUI
- [ ] Separate in-scope vs out-of-scope assets
- [ ] Document boundaries and data flows

🔐 Step 3: Implement Required Controls

- [ ] For Level 1: Apply 17 basic safeguarding practices (FAR 52.204-21)
- [ ] For Level 2: Implement all 110 NIST SP 800-171 controls
- [ ] Ensure policies and procedures are documented and enforced

🧠 Step 4: Prepare for Assessment

- [ ] Create a **System Security Plan (SSP)**
- [ ] Build a **Plan of Action & Milestones (POA&M)** for any gaps
- [ ] Conduct internal reviews or mock assessments
- [ ] Submit **Level 1 self-assessment** to SPRS (if applicable)

🖱️ Step 5: Maintain Readiness

- [ ] Train staff on security awareness and CUI handling
- [ ] Monitor systems and log security events
- [ ] Update documentation and controls regularly
- [ ] Stay informed on DoD and CyberAB updates