✅ NIST SP 800-171 Level 1 Checklist

Basic Safeguarding of Controlled Unclassified Information

🔐 1. Access Control (AC)

Goal: Limit access to authorized users only.

- ☐ Do all users have unique logins (no shared accounts)
- ☐ Are basic session locks enabled (screen lock after inactivity)
- ☐ Are remote access methods limited and controlled (e.g., VPN, if available)

🧭 2. Awareness & Training (AT)

Goal: Ensure users understand basic security responsibilities.

- ☐ Do users understand phishing, password hygiene, and safe data handling

🖥️ 3. Audit & Accountability (AU)

Goal: Enable basic tracking of system activity.

- ☐ Are system logs enabled by default (Windows, M365, etc.)
- ☐ Are logs retained for a reasonable period (30–90 days minimum)

(Level 1 does NOT require full SIEM or log review programs — just basic logging.)

🛡️ 4. Configuration Management (CM)

Goal: Maintain secure baseline configurations.

- ☐ Are systems kept up to date with vendor patches
- ☐ Are unnecessary accounts, services, and software removed
- ☐ Are antivirus/EDR tools installed and active or Windows Defender

🔧 5. Identification & Authentication (IA)

Goal: Verify user identity before granting access.

- ☐ Are strong passwords enforced
- ☐ Are unique user accounts used for all access
- ☐ Is MFA enabled wherever possible (email, cloud apps, VPN)

🔒 6. Physical Protection (PE)

Goal: Prevent unauthorized physical access to systems storing FCI.

- ☐ Are offices, server rooms, and storage areas locked
- ☐ Are laptops and mobile devices secured when unattended
- ☐ Are paper records stored securely

🌐 7. System & Communications Protection (SC)

Goal: Protect data in transit and at system boundaries.

- ☐ Are firewalls enabled on all devices
- ☐ Are wireless networks secured (WPA2/WPA3, strong passphrases)
- ☐ Is guest Wi-Fi separated from business systems

🛠️ 8. System & Information Integrity (SI)

Goal: Detect and address basic cybersecurity threats.

- ☐ Is antivirus/EDR installed and updated automatically
- ☐ Are systems patched regularly
- ☐ Are users trained to report suspicious activity
- ☐ Are email filters and spam protection enabled

📄 Optional but Recommended

Even though Level 1 doesn’t require heavy documentation, Bradley Defense is happy to provide your company a 1 to 2 Cybersecurity Policy upon request