Readiness Checklist For DoD Subcontractors

This checklist is designed to help defense subcontractors prepare for CMMC Level 1 or Level 2 compliance. It aligns with NIST SP 800-171 requirements and outlines the key steps required before a formal assessment.

1. Determine Your Required CMMC Level

- Review current DoD contracts and flow-down clauses.
- Identify whether you handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).
- Confirm whether DFARS 252.204-7012 applies.
- Document required CMMC level (Level 1 or Level 2).

2. Define Compliance Scope

- Identify all systems storing or processing CUI.
- Inventory endpoints, servers, and network infrastructure.
- Review cloud environments (Microsoft 365, Azure, GCC, etc.).
- Identify third-party vendors with system access.
- Document system boundaries.

3. Conduct NIST 800-171 Control Review

- Review all 14 control families.
- Evaluate implementation of 110 security controls (Level 2).
- Document control ownership and implementation status.
- Collect evidence for each implemented control.

4. Perform CMMC Self Assessment

- Use a structured CMMC self assessment checklist.
- Score each control as implemented, partially implemented, or not implemented.
- Identify missing policies and technical safeguards.
- Create preliminary findings report.

5. Complete Gap Analysis

- List controls requiring remediation.
- Prioritize high-risk deficiencies.
- Develop Plan of Action and Milestones (POA&M;).
- Estimate remediation timelines and resources.

Informational resource only – not certification guidance.

6. Implement Required Security Controls

- Deploy multi-factor authentication across all systems.
- Implement endpoint detection and response.
- Encrypt data at rest and in transit.
- Configure secure access controls and least privilege access.
- Enable logging and monitoring capabilities.

7. Develop Required Documentation

- Create or update System Security Plan (SSP).
- Document Incident Response Plan.
- Develop Access Control and Configuration Management policies.
- Conduct formal risk assessment documentation.
- Maintain employee security awareness training records.

8. Validate Readiness Before Assessment

- Test incident response procedures.
- Review user access permissions.
- Confirm backup and recovery processes.
- Verify audit log retention.
- Organize evidence repository.

9. Prepare for Third-Party Assessment (If Required)

- Confirm assessment requirement for Level 2 certification.
- Assign internal compliance coordinator.
- Prepare documentation index for assessor review.
- Conduct pre-assessment readiness review.

10. Prepare and Submit Your SPRS Score

Many Department of Defense contracts require contractors to submit a NIST SP 800-171 self-assessment score to the Supplier Performance Risk System (SPRS).

- Calculate your NIST 800-171 assessment score using the DoD scoring methodology.
- Document the date of assessment and responsible organization.
- Maintain your System Security Plan (SSP) and supporting documentation.
- Submit the score through the SPRS portal if required by contract.
- Update the score after major remediation activities.

Maintaining an accurate SPRS score is often a prerequisite for contract eligibility.

Notes and Internal Tracking

Use this section to record control ownership, remediation status, deadlines, and internal review notes. Maintaining clear documentation is critical for successful CMMC certification.

Disclaimer

This document is provided for informational and educational purposes only. It is not intended to serve as legal advice, regulatory guidance, or formal certification preparation. CMMC certification assessments must be performed by an authorized C3PAO. Secure Networks ITC makes no guarantees regarding certification outcomes and assumes no responsibility for any actions, decisions, or business impacts resulting from the use of this checklist. Organizations should consult qualified compliance, legal, or cybersecurity professionals when preparing for CMMC certification.