CyberFoundry

CMMC 2.0 Level 2 Pre-Assessment Scoping Exercise

Pre-Engagement Questions

Purpose: These questions are designed to help us understand at a high level whether CMMC Level 2 applies to your organization and how broad your potential assessment scope may be.

Please keep answers brief; detailed follow-up will happen during a formal engagement.

Contract & Data Exposure

1. Do you currently hold, or expect to hold, DoD contracts that involve handling Controlled Unclassified Information (CUI) (e.g., drawings, specifications, technical data)?
2. If unsure, have you received markings on any contract documents (e.g., "CUI," "Export Controlled," "FOUO")?
3. If you only handle Federal Contract Information (FCI) (basic order details, schedules, non-public but not technical), please note that.

Current Compliance Posture

1. Have you submitted a NIST SP 800-171 self-assessment score in the Supplier Performance Risk System (SPRS)?
2. Do you currently have a System Security Plan (SSP) or equivalent cybersecurity documentation?
3. Do you maintain a list of open Plan of Action & Milestones (POA&Ms) for security gaps?

Systems & Boundaries

1. Do you maintain a separate network or enclave for defense work, or is it integrated with your corporate IT?
2. Do you have manufacturing, OT, or test equipment connected to your IT network that is used for DoD programs?
3. Do you use cloud services (e.g., Microsoft 365, Google Workspace, CAD/CAM SaaS) to process or store DoD data?

External Partners

1. Do you rely on external service providers (e.g., IT managed services, SOC/NOC, hosted file exchange) that might see or handle DoD information?

2. Do you have contracts or evidence from those providers showing they meet FedRAMP Moderate equivalency or CMMC/NIST 800-171 requirements?

Organizational Awareness

1. Has senior leadership been briefed on CMMC obligations and the difference between Level 1 (FCI) and Level 2 (CUI)?
2. Do you have an internal point of contact (compliance manager, IT/security lead) responsible for CMMC readiness?
3. Have you budgeted or planned for CMMC activities in the next 12–24 months?

CyberFoundry

CMMC 2.0 Pre-Assessment Scoping Exercise

Pre-Engagement Artifact Collection

Purpose: The information requested below is what we need to properly complete the CMMC Level 2 Scoping Guide. It will be used in our pre-assessment discussions and again when preparing your official scoping documentation. You may not have all of this available today, and that's normal at this stage. However, before your organization can formally become an Organization Seeking Certification (OSC), this evidence will need to be complete and validated. Not having it now may create uncertainty in your defined scope and may create delays or additional expense in preparing your scoping documentation.

Contracts & Data Classification

- Sample DoD contract / task order / subcontract language showing if CUI is expected.
- Examples of marked documents (drawings, specs, technical data) with "CUI," "Export Controlled," or similar markings.
- Contract flow-down clauses (DFARS 252.204-7012/7019/7020) included in PO/SOW.

Asset Inventory & Diagrams

- Complete asset inventory (hardware, software, OT, test equipment).
- Designation of each asset as CUI Asset, Security Protection Asset (SPA), Contractor Risk Managed Asset (CRMA), Specialized, or Out-of-Scope.
- Network diagram(s) — logical and physical — showing enclaves, VLANs, firewalls, VPNs, wireless, external connections.
- Data flow diagram(s) showing how CUI enters, moves, and exits the environment (from receipt to disposition).

System Security Documentation

- System Security Plan (SSP) (draft or current).
- SPRS NIST 800-171 self-assessment score and date of submission.
- POA&M list (if any) identifying open gaps and planned remediation.

Security Protection Assets (SPAs)

- Firewall/router configs protecting CUI enclaves.
- SIEM/log server inventory showing they capture and protect CUI-related logs.

- Endpoint detection/anti-virus tooling inventory.
- Identity management systems (AD, Azure AD, IAM service).

Contractor Risk-Managed Assets (CRMAs)

- List of systems "capable but not used" for CUI (e.g., corporate email, ERP).
- Policies/procedures that prohibit CUI use on those systems.
- Validation evidence (spot checks, DLP, or technical controls showing CUI segregation).

Specialized Assets

- List of OT/test equipment (CAM workstations, CNC, PLCs, oscilloscopes, test rigs).
- Segmentation/isolation evidence (air-gaps, VLAN, firewall rules).
- Vendor docs for restricted or government-furnished equipment (GFE).
- Exception rationale if requesting "enduring exceptions" under the Scoping Guide.

External Service Providers (ESPs) / Cloud

- Contracts/SOWs with ESPs (managed IT, MSSP, SOC, etc.).
- FedRAMP Moderate equivalency evidence from cloud providers (Microsoft GCC High, AWS GovCloud, etc.).
- Customer Responsibility Matrices (CRMs) showing shared control responsibilities.
- Service descriptions / SLAs documenting who owns what controls.

Boundary & Separation

- Policies/diagrams showing logical or physical separation of CUI vs non-CUI systems.
- Firewall/VLAN configs documenting enforced segmentation.
- Access control lists (who can cross boundaries, remote access configs).
- Information flow control policy (what data is allowed across enclaves).

Incident Reporting & IR Preparedness

- Incident Response Plan (with 72-hour DoD reporting workflow).
- Evidence of DIBNet account/registration for incident reporting.
- Forensic retention policy (logs, images, artifacts).

Governance & Awareness

- Policy statements assigning responsibility for CUI handling.
- Training records showing users are briefed on CUI vs FCI and marking/handling.
- Org chart or POC list — who owns CMMC readiness, IT, compliance, and incident response.