



FREE CHECKLIST

# CMMC Preparation: What to Gather Before You Start

A checklist for small defense contractors: the documents, facts and people to pull together so you know where you stand.

## INSIDE

9 areas to gather · the DFARS clauses to look for · a starting-point summary sheet

balancelogic.com · 301-396-8455



## WHY GATHER FIRST

The first weeks of most Cybersecurity Maturity Model Certification (CMMC) preparation go to hunting for things: contracts, diagrams, old policies, a half-remembered Supplier Performance Risk System (SPRS) score. Gather them first and the time goes to decisions instead.

This checklist is for small defense contractors and subcontractors that handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI). Work through it with whoever knows your contracts, your systems and your IT setup. You don't need everything to be finished or perfect. The goal is to know where you stand today, and to give your Affirming Official the facts they need before signing an affirmation of compliance.

**Focus on what you control.** Program timelines can change. The clauses in your current contracts, the information you actually hold, and the affirmation your company signs don't depend on them. Check each new solicitation for the requirements that apply to it.

## 1. Contracts and clauses

Pull your current prime contracts, subcontracts and purchase orders, plus any open solicitations you plan to bid. Search each one for these Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) clauses. Several point to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, the security requirements for protecting CUI.

| Clause                    | Title                                                                                        | What to note                                                                                                     | Found?                   |
|---------------------------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|--------------------------|
| <b>FAR 52.204-21</b>      | Basic Safeguarding of Covered Contractor Information Systems                                 | You hold FCI and must apply its basic safeguarding requirements.                                                 | <input type="checkbox"/> |
| <b>DFARS 252.204-7012</b> | Safeguarding Covered Defense Information and Cyber Incident Reporting                        | You may hold CUI. It requires NIST SP 800-171, 72-hour incident reporting and cloud provider requirements.       | <input type="checkbox"/> |
| <b>DFARS 252.204-7019</b> | Notice of NIST SP 800-171 DoD Assessment Requirements                                        | A current NIST SP 800-171 assessment score is expected in SPRS to be considered for award.                       | <input type="checkbox"/> |
| <b>DFARS 252.204-7020</b> | NIST SP 800-171 DoD Assessment Requirements                                                  | Assessment and SPRS posting requirements, and flowdown to your subcontractors.                                   | <input type="checkbox"/> |
| <b>DFARS 252.204-7021</b> | Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements | Which CMMC level the contract requires, annual affirmations in SPRS, and reporting your CMMC unique identifiers. | <input type="checkbox"/> |

☐ For each contract, we've noted which clauses appear, the CMMC level required (if stated), and the contracting officer or prime contractor contact.

☐ We've checked the subcontracts we issue, and know which of our own suppliers receive FCI or CUI from us.

These clauses flow down. Your suppliers may need their own scores and affirmations.

☐ We've kept a copy of any CUI guidance, marking instructions or security requirements the customer sent with the contract.

Clause titles and requirements checked against the eCFR ([ecfr.gov](https://www.ecfr.gov)): 48 CFR 52.204-21, 48 CFR 252.204-7012, -7019, -7020 and -7021, and 32 CFR 170.4. Read the clause version in your own contract.

## 2. The information you receive and where it lives

---

Your scope depends on where FCI and CUI actually go. Follow the information, not the org chart.

☐ We've listed what we receive from the government or our primes: drawings, specifications, technical data, reports, contract documents.

☐ For each, we know whether it's marked as CUI, and who told us how to handle it.  
If you aren't sure whether something is CUI, ask the contracting officer or prime in writing and keep the answer.

☐ We know how it arrives: email, a customer portal, file transfer, removable media, paper.

☐ We know everywhere it goes next: email inboxes, file shares, laptops, engineering or design systems, backups, printers, phones, paper files.

☐ We know who outside the company receives it from us, such as suppliers, machine shops or consultants.

☐ We know which people actually work with CUI day to day, and roughly how many.

## 3. Asset and system inventory

---

☐ A list of every computer, server, phone and tablet that can access FCI or CUI, with its owner and location.

☐ Network equipment: firewalls, switches, wireless access points, VPN devices.

☐ Software and systems that store or process CUI, including engineering, manufacturing and ERP systems.

☐ Specialized equipment that touches CUI, such as CNC machines, test equipment or scanners.

☐ User accounts, including shared and administrator accounts, and who approves new ones.

- ☐ Anything personally owned that's used for work, such as personal phones that receive company email.

## 4. Network and data-flow diagrams

---

- ☐ A current network diagram showing offices, internet connections, firewalls, wireless networks and remote access.  
A clear hand drawing that's accurate beats a polished diagram that's out of date.
- ☐ A data-flow diagram showing how CUI comes in, where it's stored and processed, and how it leaves.
- ☐ Any boundary you've already drawn around the systems that handle CUI, and how it's separated from everything else.
- ☐ Connections to outside parties: customer portals, cloud services, your IT provider's remote tools.

## 5. Existing policies and documents

---

Gather what exists, even if it's old or incomplete. Note the date and owner of each.

- ☐ System Security Plan (SSP), if you have one.
- ☐ Plan of Action and Milestones (POA&M) for gaps you've already identified.
- ☐ Information security, acceptable use and access control policies.
- ☐ Incident response plan and any records of past incidents.
- ☐ Security awareness training records.
- ☐ Onboarding and offboarding procedures, and background check practices.
- ☐ Backup, media handling and disposal procedures.
- ☐ Physical security: visitor logs, badge or key controls, alarm records.
- ☐ Any previous assessments, audits or questionnaires you've completed for customers.

## 6. Your current SPRS status

---

SPRS is where the Department of Defense (DoD) sees your NIST SP 800-171 assessment score and CMMC affirmations. For a Basic self-assessment, your company submits its own score. DoD posts the results of Medium and High assessments, which it conducts itself.

- ☐ We know whether a score has been posted for our company, and who has access to view it in SPRS.

- ☐ We know the score, the date of the assessment, and the NIST SP 800-171 version it was based on.
- ☐ We know who performed the assessment and who submitted it, and we have the working papers behind the number.

The score is only as good as the evidence behind it. If no one can explain how it was reached, treat it as unknown.
- ☐ We know which CAGE codes the score covers, and whether it covers all the systems that handle CUI.
- ☐ We know whether the score is still current. DFARS 252.204-7019 treats an assessment as current if it is not more than three years old, unless the solicitation sets a shorter period. DFARS 252.204-7020 applies the same three-year test to subcontractors.
- ☐ We know the date our POA&M says we'll reach full implementation, and whether that's still realistic.

## 7. The people involved

---

- ☐ **Owner or executive sponsor:** someone with the authority to approve time, budget and priorities.
- ☐ **Affirming Official:** the senior person who will affirm the company's compliance in SPRS. Under 32 CFR 170.4, this is the senior level representative responsible for ensuring compliance and with authority to affirm continuing compliance.

They should understand what they are signing and see the evidence before they sign it.
- ☐ **IT lead:** your internal IT person or your current MSP, and the name of the person there who knows your environment.
- ☐ **Contracts lead:** whoever reads the contracts and talks to contracting officers and primes.
- ☐ **Operations, engineering and HR contacts:** the people who handle CUI daily, and whoever manages hiring, onboarding and departures.
- ☐ **Facilities contact:** whoever controls building access, visitors and physical records.

## 8. Cloud services used for CUI

---

- ☐ A list of every cloud service that stores, processes or transmits CUI: email, file sharing, collaboration, backup, engineering or ERP platforms.
- ☐ For each, which version or plan you use, since government and commercial versions of the same product can differ.
- ☐ Evidence that each provider meets the security requirements DFARS 252.204-7012 sets for cloud services holding covered defense information, equivalent to the FedRAMP Moderate baseline.

Ask the provider for its documentation. A marketing page isn't evidence.

- ☐ Your provider's commitments on incident reporting, and on preserving and giving access to data if there's an incident.
- ☐ Any cloud services staff use on their own, such as personal file-sharing accounts, that may have received CUI.

## 9. Incident reporting contacts

- ☐ We know DFARS 252.204-7012 requires reporting a cyber incident affecting covered defense information to DoD within 72 hours of discovery, through [dibnet.dod.mil](https://dibnet.dod.mil).
- ☐ We know who in the company makes and files that report, and who backs them up.
- ☐ We have the DoD-approved medium assurance certificate needed to file a report, or know how we'd get one quickly.  
Getting a certificate takes time. Don't leave it until you're in the middle of an incident.
- ☐ We have current contacts for our contracting officers and primes, our IT provider, our cyber insurer, and legal counsel.
- ☐ Staff know how to report a suspected incident internally, and to whom.

## Your starting point

Summarize what you found. "Partial" is a normal answer for most of these.

| Item                                       | Have                     | Partial                  | Missing                  | Owner | Where stored |
|--------------------------------------------|--------------------------|--------------------------|--------------------------|-------|--------------|
| Contracts and clauses reviewed             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |       |              |
| FCI and CUI identified and located         | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |       |              |
| Asset and system inventory                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |       |              |
| Network and data-flow diagrams             | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |       |              |
| Policies, SSP and POA&M                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |       |              |
| SPRS score and evidence                    | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |       |              |
| People named, including Affirming Official | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |       |              |
| Cloud services for CUI documented          | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |       |              |
| Incident reporting ready                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |       |              |

## What comes next

---

With this information in hand, the next step is a structured review against NIST SP 800-171, before any certification assessment by a Certified Third-Party Assessment Organization (C3PAO) that your contracts require. The Balancelogic CMMC Readiness Review runs in three phases. Each phase has a fixed scope and clear deliverables, so you can start with Phase 1 and decide on the next step with real information.

**Phase 1: Assessment & Roadmap.** We review your environment against NIST SP 800-171, define your CUI boundary, and identify the gaps. You get a prioritized roadmap: what to fix, in what order.

You submit your SPRS score. We help you prepare the score and the supporting documentation. Certification assessments are conducted by an authorized third party, such as a C3PAO. The Balancelogic CMMC Readiness Review prepares you for it.

---

Our work supports your compliance program. It doesn't guarantee compliance, certification, or assessment results.

### Ready to find out where you stand?

Not sure which CMMC requirements apply to you yet? Send us a message and ask about a Balancelogic CMMC Readiness Review.

[balancelogic.com/contact-us](https://balancelogic.com/contact-us) · 301-396-8455 · 3825 Leonardtown Road, Suite 5, Waldorf, MD 20601