

Federal Contract Information (FCI)

FCI is information that:

- Is provided by the Government under a contract, or
- Is generated for the Government under a contract,
- And is not intended for public release.

This definition comes from:

- 32 CFR § 170.4 (CMMC Program rule)
- 48 CFR 4.1901
- CMMC Model Overview v2.13, Section 1 (definition of FCI)

Under CMMC Level 1, any system that processes, stores, or transmits FCI must meet the 15 basic safeguarding requirements in FAR 52.204-21.

Examples of FCI

These are common examples in defense contracts:

- Statements of Work (SOWs)
- Contract deliverables
- Technical drawings provided under contract
- Internal reports created for the Government
- Contract performance schedules
- Non-public Government emails related to the contract
- Non-public project status updates
- Non-public pricing or cost breakdowns tied to contract work

If it exists because of the contract and isn't public, treat it as FCI.

For a visual overview, refer to the FCI Determination Workflow.

What is NOT FCI?

The definition specifically excludes two major categories:

Public Information

If the information is intended for public dissemination, it is NOT FCI.

Examples:

- Information on official Government websites
- Press releases
- Publicly released contract awards
- Public technical data

If anyone can access it without restriction, it is not FCI.

Simple Transactional Information

Basic administrative information needed only to process payments or routine business is NOT FCI.

Examples:

- Invoice numbers
- Payment processing information
- Shipping tracking numbers
- Basic billing correspondence

If it's just administrative processing data and not substantive contract content, it is not FCI.

What is needed for CMMC Level 1?

If your company receives Federal Contract Information (FCI), you must follow 15 basic cybersecurity safeguards under FAR 52.204-21 and [complete an annual CMMC Level 1 self-assessment](#).

These are not advanced security controls. They are common-sense protections that are generally in place for any business.

For detailed information on each of the 15 basic cybersecurity safeguards, see the CMMC Level 1 Requirements Table.