Understanding FAR vs DFARS: Key Differences for DoD Contract Compliance

When you start working with Department of Defense contracts, two sets of regulations quickly become familiar: the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS). At first glance they look like a single dense block of rules. But anyone who has managed a DoD contract for more than a few months learns that the distinction matters a lot. I have seen teams waste weeks because they treated DFARS requirements as optional or assumed FAR clauses covered everything. The difference is not academic. It affects how you handle data, who you hire, what software you can use, and how much you can bill.

The FAR is the baseline. It applies to all federal agencies. DFARS is the supplement that the Department of Defense adds on top. If you think of the FAR as the foundation of a house, DFARS is the extra bracing, fireproofing, and security systems that the DoD requires because its work is more sensitive. The relationship is hierarchical. Where DFARS speaks, it overrides or adds to the FAR. Where it is silent, the FAR controls. Understanding this relationship is the first step. But the real challenge is knowing which parts of DFARS apply to your specific contract and which do not.

Why the Distinction Exists

The DoD buys things that most agencies do not: weapons systems, classified equipment, intelligence services, and items that must survive battlefield conditions. The FAR alone cannot address these needs. DFARS fills the gaps. It covers areas like contractor purchasing systems reviews, cost accounting standards for defense contracts, and the safeguarding of unclassified controlled technical information. If you are a commercial supplier used to selling simple office supplies, DFARS may barely touch you. But if you build software for a missile program, you will live inside DFARS clauses.

I once worked with a small manufacturing firm that had a single DoD contract to produce spare parts for a ground vehicle. The owner assumed that because the contract was small, DFARS did not apply. He was wrong. The contract included DFARS clause 252.204-7004, which required a compliant purchasing system. He had to redesign his procurement process and undergo a system review. That experience taught me that you cannot guess which DFARS clauses apply. You have to read the contract and the incorporated clauses carefully.

The Core Differences at a Glance

Rather than listing every clause, it helps to understand the areas where DFARS diverges most sharply from the FAR. The following points capture the practical differences that contractors encounter most often.

- **Scope of application:** FAR governs all federal acquisitions. DFARS applies only to DoD contracts and subcontracts.
- **Data rights and intellectual property:** DFARS has stricter rules about the government's rights to technical data and computer software developed with federal funds.
- **Cybersecurity:** DFARS mandates compliance with NIST SP 800-171 for any contractor handling controlled unclassified information. The FAR does not impose this requirement across all agencies.
- **Cost accounting:** DFARS requires more detailed cost accounting and disclosure statements for larger contracts, especially those that are cost-type.
- **Purchasing systems:** DFARS requires contractors to maintain an approved purchasing system and undergo periodic reviews, something rare outside the DoD.

These are not minor differences. A contractor who treats a DFARS requirement as a suggestion may end up with a withheld payment, a suspension, or worse. I have seen companies lose existing contracts because they assumed their FAR-compliant processes automatically satisfied DFARS. They did not.

When the Difference Hits Home: Cybersecurity and Data Handling

Of all the areas where far vs dfars matters most, cybersecurity is the one that keeps contractors up at night. Under the FAR, cybersecurity requirements are relatively light for most commercial items. Under DFARS, the requirement to implement NIST SP 800-171 is now standard. The Defense Federal Acquisition Regulation Supplement clause 252.204-7012 mandates that contractors provide adequate security for covered defense information and report cyber incidents to the DoD within 72 hours.

I have seen small businesses panic when they realize their IT infrastructure does not meet these standards. One engineering firm I consulted for had all its design files on a shared drive with no encryption and no multi-factor authentication. They had been doing business with the DoD for three years without a problem. Then a new contract included the DFARS cybersecurity clause. They had to spend six months and over forty thousand dollars to bring their systems into compliance. That cost could have been avoided if they had understood the far vs dfars dynamic earlier.

The key takeaway here is that DFARS cybersecurity requirements are not optional. They are flow-down requirements. If you are a subcontractor, your prime contractor will pass them down

to you. You cannot negotiate your way out of them. The only way to handle them is to build compliance into your operations from the start.

Practical Steps for Managing Both Regulations

Over the years I have developed a short list of practices that help contractors avoid the common pitfalls. These are not theoretical. They come from watching people succeed and fail.

1. **Know which clauses are in your contract.** The government does not always use the same set of DFARS clauses. Check the contract's list of incorporated clauses and read them. Do not rely on memory.
2. **Flow DFARS requirements to your subcontractors.** If you are a prime, you are responsible for your whole supply chain. Write DFARS clauses into your subcontracts and verify compliance.
3. **Use a compliance checklist.** Build a matrix that maps each DFARS clause to a specific process or document in your company. Update it every contract period.
4. **Invest in your purchasing system early.** Even if you do not think you need a formal system, having one saves you from a later review.
5. **Train your team.** The people who write proposals, handle data, and manage subcontracts need to know the basics of DFARS. One person cannot carry the whole load.

These steps are not revolutionary, but they work. I have seen companies with fewer than fifty employees handle DFARS compliance smoothly because they followed a disciplined approach. I have also seen large companies stumble because they assumed their size would protect them. It does not.

Common Misconceptions

One misconception is that DFARS only applies to large prime contractors. That is false. DFARS flows down to subcontractors at every tier. Another is that commercial items are exempt from DFARS. They are not entirely. The government can still impose DFARS clauses on commercial items, especially for cybersecurity and data rights. A third misconception is that once you comply with the FAR, DFARS compliance is automatic. As I have already shown, that is not true. The FAR does not require NIST SP 800-171. The FAR does not require a purchasing system review. The FAR does not require cost accounting standards specific to the DoD.

The truth is simpler. You have to treat DFARS as its own body of law. The FAR is the floor. DFARS is the ceiling. You live somewhere in between, and the specific contract tells you where.

Final Thoughts

Working with DoD contracts is rewarding but demanding. The regulations exist for a reason. They protect national security, ensure fair pricing, and hold contractors accountable. The challenge is not that the regulations are bad. It is that they are dense and easy to misinterpret. The difference between far vs dfars is not a trivia question. It is a practical distinction that affects every decision you make on a defense contract. Take the time to learn it. Your budget, your reputation, and your eligibility for future contracts depend on it.