Understanding Government Contracting Requirements for DFARS Compliance

Working with the Department of Defense (DoD) has its own rhythm. When I first started submitting proposals for defense contracts, I assumed the hardest part was writing a strong technical proposal. It turns out that understanding government contracting requirements is what separates the firms that win from the ones that constantly protest. The rules are thick, the terms are precise, and one misstep can delay a contract by months. Over the past decade, I have watched companies stumble over the same basic compliance gaps. The good news is that most of these requirements are learnable, and the effort you put into understanding them pays off in fewer rejected bids and smoother contract administration.

What Makes DFARS Compliance Different

DFARS stands for the Defense Federal Acquisition Regulation Supplement. If you have ever worked with federal procurement, you know the Federal Acquisition Regulation (FAR) is the baseline. DFARS adds another layer specific to the DoD. It covers everything from cybersecurity standards to cost accounting rules. Many contractors treat DFARS as an afterthought, but that is a mistake. The DoD has become aggressive about auditing compliance, especially for small and medium businesses that might not have dedicated compliance teams.

One of the first things I tell new contractors is that government contracting requirements include both the obvious clauses and the hidden ones. For instance, if you handle any covered defense information, you need to comply with DFARS clause 252.204-7012. That clause demands specific security controls. I have seen a company lose a twenty-million-dollar contract because they did not have a System Security Plan in place. The DoD does not always give you a chance to fix things after award. They check before they sign.

Security and Data Protection

Cybersecurity is the most discussed part of DFARS right now. The DoD requires contractors to implement the NIST SP 800-171 controls for any system that processes, stores, or transmits covered defense information. That is a list of 110 security requirements spread across fourteen families. For a small business, this can feel overwhelming. But the DoD has provided a self-assessment tool called the Supplier Performance Risk System (SPRS). You submit your score there, and the DoD uses it as part of their award decisions.

I once worked with a manufacturer that had never done a self-assessment. They had good security practices but no formal documentation. We spent two weeks mapping their controls to the NIST framework. They scored moderately, but the benefit was that they could see exactly

where their gaps were. They fixed the gaps over the next year and moved from a non-compliant status to a compliant one. That improvement helped them win several follow-on contracts.

Cost Accounting Standards

Another area where government contracting requirements get tricky is cost accounting. The DoD demands that contractors use a consistent and auditable method for allocating costs to contracts. If you are a commercial company used to a single overhead pool, you might need to switch to a job-costing system. The rules require that you separate direct costs from indirect costs and that you allocate indirect costs using a base that reflects the actual benefit each contract receives.

I have seen companies get into trouble because they used a simple percentage split that did not match the actual work. The Defense Contract Audit Agency (DCAA) reviews these allocations, and if they find them unreasonable, they can disallow costs. That means you might not get paid for work you already performed. The fix is to set up your accounting system early. Talk to a DCAA-compliant accountant before you submit your first cost-type proposal. It will save you hours of rework later.

Flow-Down Clauses

Many prime contractors think they can handle compliance on their own. But if you are a subcontractor, you also need to understand the requirements. The prime flows down clauses to you. If your prime has a DFARS clause in their contract, you likely have the same obligation in your subcontract. I have seen subcontractors ignore these clauses because they assumed the prime would handle everything. That is not how it works. If the DoD audits the prime, they ask to see your compliance evidence too.

One practical step is to keep a copy of every flow-down clause you receive. Compare it against the DFARS requirements. If you see a clause that requires a specific certification, make sure your compliance team has a plan to meet it before you start work. The worst time to discover a gap is during a DCAA audit.

Common Pitfalls and How to Avoid Them

Over the years, I have noticed a few patterns that cause repeated problems. Here are the three most common:

- **Missing documentation.** Many contractors have good practices but no written policies. The DoD expects written policies, especially for cybersecurity and ethics. Write them down, even if they seem basic.

- **Assuming small contracts are exempt.** Some contracting officers treat every contract seriously. Even if you have a small purchase order, you still need to comply with applicable clauses. Ignoring them because the dollar value is low is risky.
- **Not training employees.** Your compliance program is only as strong as your people. If your engineers do not know the security controls, they will accidentally expose data. Regular training is not optional.

Structuring Your Compliance Program

Building a compliance program from scratch sounds daunting, but you do not need to reinvent the wheel. Start by identifying which DFARS clauses apply to your contracts. The easiest way is to look at the clauses listed in your solicitation or contract. Then map each clause to a specific action: a policy to write, a control to implement, or a report to file. Create a simple checklist and update it every time you bid on a new contract.

I recommend assigning one person on your team to own compliance. That person does not need to be a lawyer, but they should be methodical. They need to track deadlines for submitting cost proposals, updating security plans, and responding to audits. Many companies fail not because they cannot comply, but because they forget to submit the paperwork in time. A calendar with reminders can be the difference between a compliant proposal and a rejected one.

What to Expect During an Audit

Audits are a normal part of defense contracting. The DoD and the DCAA conduct them to verify that you are meeting government contracting requirements. The process usually starts with a letter or email requesting specific documents. They might ask for your accounting records, your cybersecurity self-assessment score, or your purchasing system policies. The key is to respond promptly and completely. If you delay, they assume you are hiding something.

I once sat through a DCAA audit that lasted three days. The auditor went through every cost allocation and every invoice. Because we had kept clean records, the audit went smoothly. The auditor even complimented our documentation. That is the goal. Not just to survive an audit, but to make it look easy. That reputation spreads. Prime contractors remember who handles audits well.

Balancing Compliance with Business Growth

One concern I hear often is that compliance slows down business. There is some truth to that. Setting up a compliant system takes time and money. But the alternative is worse. If you win a contract and then fail an audit, you can lose the contract and your reputation. The DoD

maintains a database of debarred contractors. Getting on that list is a career-ending event for most small firms.

I advise companies to view compliance as a competitive advantage. When you can show a prime that you already have a compliant system, you become a more attractive partner. They do not have to hand-hold you through the process. You can start work faster and with less risk. That trust translates into more subcontracts and stronger relationships.

Final Thoughts

Navigating government contracting requirements is not a one-time task. It is a continuous process of learning, updating, and auditing. The DoD changes its regulations periodically, so you need to stay informed. I subscribe to a few industry newsletters and attend webinars whenever I can. That keeps me ahead of the curve.

If you are just starting out, do not try to master everything at once. Focus on the most common requirements first: cybersecurity, cost accounting, and flow-down clauses. Once those are solid, move on to the more specialized areas like property management or environmental compliance. Step by step, you build a system that keeps you compliant and competitive.

The companies that succeed in defense contracting are the ones that respect the rules without being intimidated by them. They see compliance as part of the job, not an obstacle. With the right approach, you can join them.