Once again we post *yet another* article blathering on about subcontractor/supplier management and how important it is to program execution. You'd think we'd get off that particular soapbox after six years, right? Seen it; read it; no need to see it or read it again. *Boring!*

A couple of weeks ago we were privileged to speak at the Public Contracting Institute's annual "DCAA Hot Topics" update seminar, held in Dallas, Texas. The topic was the DFARS Business Systems but we chose to focus on moving beyond the "first line of defense against fraud, waste, and abuse" and, instead, addressed the compliance risks that the six "first lines" don't address. (Indeed, as you know if you are any kind of reader of this blog, we don't think those six systems do much of anything at all with respect to detecting or preventing fraud, waste, or abuse.) We spoke about compliance risks that exist outside the walls of the contractor's facility: the compliance risks that exist in the program's supply chain.

Again, a topic that we've discussed and written about before. Not much new to say or to write about it, right?

And as we've noted before, attorneys have a tendency to want to protect their corporate client(s) by focusing on contract language that protects and perhaps indemnifies the client from any wrongful actions performed by the subcontractors/suppliers in that program supply chain. We've even seen the phrase "transfer of risk from prime to sub" used before – and it bothered us. It bothered us because you can't do that. You cannot transfer risk from prime contractor to subcontractor and there is no contract language that will do so. The most you can do is to put language in your agreement that will make the prime whole from the actions of its suppliers; and even then the phrase "make the prime whole" is problematic, because there are some things (such as schedule slips to significant program milestones) from which the program cannot recover.

Thus: our asserted position that program execution risk cannot be transferred and attorneys who believe otherwise simply do not understand what the phrase "program execution" actually means.

Enough rehashing of points made previously in other blog articles. Where are we going with this? Well, we're going to make a relatively new point today:

Prime contractors (and higher-tier subcontractors) cannot simply rely on contract language to protect themselves from the wrongdoing of their suppliers and subcontractors. They cannot simply rely on certifications and representations. Prime contractors (and higher-tier subcontractors) will be held accountable for the wrongdoing of their suppliers.

Accordingly, they need to actually verify the representations and certifications. They need to actually review, audit, and/or confirm the assertions made by their suppliers.

*That's a **bold** set of statements*, we hear you saying. Expensive, too. And manpower-intensive as well. Not likely to happen in this budget-conscious age of cost-cutting and layoffs.

But we think we are correct. Contractors that simply accept documents and invoices at face value, without checking and verifying the accuracy of those documents and invoices, may be found to be negligent. Those negligent contractors may be subject to allegations of False Claim Act violations, with all the expense that entails. Remember, "reckless disregard" and "deliberate ignorance" have been held to meet the requisite *scienter* standard under the civil FCA statute.

Obviously, the amount of checking and verification depends on a risk analysis, and that risk analysis starts with contract type. Choosing the **correct** contract type is more important that many would think. Cost-reimbursement subcontracts require more invoice review; whereas FFP subcontracts probably require more project status report review. T&M subcontracts are just risky in every sense, and should probably be avoided if possible.

The point is: somebody needs to assess risk and then take actions that would tend to militate against the assessed risk. Program teams simply should not expect suppliers and subcontractors to do the right thing; they should be checking and reviewing and verifying that their suppliers and subcontractors are doing the right thing.

As a President once said, "Trust; but verify."

With that in mind, let's talk about CSC's prime contract with the Defense Information Systems Agency (DISA). CSC (more formally called Computer Sciences Corporation) was awarded a DISA contract to "help manage the telecommunications network" used by the Department of Defense. CSC then awarded a subcontract to NetCracker Technology Corporation. We know about this contractual relationship courtesy of the Department of Justice, which issued a **press release** describing what went wrong, the ensuing FCA litigation, and how much the two parties (CSC and NetCracker) had to pay in order to settle the allegations.

In summary, "*From 2008 through 2013, NetCracker allegedly used employees without security clearances to perform work when it knew the contract required those individuals to have security clearances, resulting in CSC recklessly submitting false claims for payment to DISA.* "

To settle the allegations, NetCracker agreed to pay $11.4 million. For its part, CSC agreed to pay $1.35 million.

Now, we all should understand why NetCracker needed to settle the FCA litigation. It provided employees that (allegedly) lacked the requisite security clearances. That's not good. A former NetCracker employee filed a *qui tam* suit (as so often happens) and then the legal process took over from there. The original relator reportedly will receive $2.359 million for his efforts. So far, so good. That's how these things work.

But what about CSC? What did it (allegedly) do wrong to lead to a $1.35 million settlement? We have no inside information, but we strongly suspect the answer lies in the sentence from the DoJ announcement that we italicized above. Notice how CSC's role was described: "CSC *recklessly* submitting false claims for payment." *Recklessly*. That's the word we think describes why CSC had to settle and why the prime contractor was even involved in the litigation.

Apparently, CSC acted recklessly when it simply paid NetCracker's invoices without checking whether or not NetCracker's employees had the required security clearances. If we are correct in our assumption, then had CSC performed any reviews or checking or verification of the security clearances of its subcontractor, then it would have had some strong defenses to the

FCA allegations of the relator. CSC didn't review or check or verify, and that lack of action cost it a (relatively small) litigation settlement.

CSC was held accountable for the wrongdoing of its subcontractor—a fact which supports the set of bold statements we made earlier in this article. NetCracker represented that its employees had the requisite security clearances. NetCracker may even have certified to that "fact" (though we suspect it was more in the nature of an "implied certification" rather than an express certification). CSC accepted NetCracker's assurances at face-value, without checking further. And that lack of diligence cost CSC $1.35 million.

Consider our assertions and the support for our assertions.

Consider not making the same mistakes as CSC.