Recently we came across **this article** , written by attorneys (and former Federal prosecutors) A. Lee Bentley III and Jason Mehta, entitled “How Contractor Fraud is Reported Shouldn’t Affect How It Gets Investigated.” The article addressed something we have pondered from time to time— *i.e.*, how does the government choose whether to pursue available administrative remedies or civil/criminal remedies?

For example, in **one article** we discussed differences between allegations of defective pricing and allegations of False Claims associated with defectively priced contracts. We wrote: “Now we have a new rule: If the Federal government detects the defective pricing, then it’s a TINA matter. But if the relator detects the defective pricing, then it’s a FCA matter. Which is inconsistent and, on its face, somewhat inequitable. But that’s the way we’re seeing it these days.”

Subsequently, we questioned that new rule when we came across allegations that BAE Systems (successor to the Stewart & Stevenson FMTV contractor) was being charged with both defective pricing and violations of the FCA—with no *qui tam* relator in sight.

Nonetheless, the DefenseOne.com article (link in the first sentence) seems to resurrect and support our initial theory. Stated simply: the government’s investigation methodology and selection of legal remedy often depends on the manner in which it learns of the alleged violation(s). The authors wrote:

The traditional way to blow the whistle is to report internally up the chain and—if that does not work—the whistleblower could report suspected wrongdoing to federal contracting officers or to Defense Department hotline numbers. When the allegations are raised up the chain, a series of investigative procedures are initiated and DOD scrutinizes the allegations with appropriate vigor. DOD has contractual rights under the Federal Acquisition Regulations to investigate these allegations, inspect the premises, review documents, and root out fraud. These administrative remedies have been a resounding success when DOD learns of instances of fraud. …

[But] when the government learns about the suspected fraud through a *qui tam* suit, the DOJ will initiate the investigation. The investigation is given the imprimatur of a “federal case” and the stakes are automatically elevated as the default remedy for a False Claims Act case is not recoupment, but rather civil penalties (recoupment plus extra money as a penalty). In addition to

the investigative steps described above, the mere fact that a whistleblower files a False Claims Act suit often results in official DOJ interviews, subpoenas and meetings.

If this hypothesis is true, if the manner in which the government learns of the allegations of wrongdoing affects both the investigatory approach and the potential legal remedies, then wouldn't you really want employees reporting their concerns to the company hotline? And if it came to that, wouldn't you really want employees reporting their concerns to the DOD Hotline? Those are the better options, right? Because, according to the article (and our experience) when an employee resorts to filing a *qui tam* lawsuit under the False Claims Act, then the company will be in for a long and *very* expensive legal journey.

And if all that is true, then doesn't that mean you really need to focus on making your company hotline as accessible to employees as possible? We mean, you *want* employees to use the hotline, right? So you need to make the entire process as user-friendly as possible. Otherwise, you risk having employees use other, less attractive means to have their concerns addressed.

What does that look like? Well, we touched on the topic in an article we **published** about 18 months ago. We wrote—

Allegations received via internal hotline should be logged. Then they should be investigated. The findings of the investigation should be summarized and the matter should be dispositioned by an independent party in accordance with applicable laws, regulations, and company procedures. Then – *and this must always happen* – the company must 'close the loop' by reporting back the disposition to the employee who made the original hotline allegations. (Obviously if the original reporter was anonymous, that's not going to happen.)

Employees who call the company hotline to report concerns are not whistle-blowers; they are concerned employees. But you can quickly convert them into whistle-blowers by ignoring their concerns or failing to report back to them the findings of your investigation. And—as we've **reported**—you cannot retaliate against any employee who avails themselves of any fraud reporting mechanism.

In fact—as that last article noted—you are required by DFARS contract clause 252.203-7002 to inform your employees, in writing, of their whistleblower rights. Of course, we are quite confident that defense contractors with that clause in their contracts have already done so. Right?

Thus, focusing on making your company hotline an attractive and user-friendly option for employees with concerns starts with education. You need to tell them about it. For certain defense contractors, you need to tell them about it in writing. But for the rest, perhaps an email blast will be sufficient. Let them know that you *want* them to use the hotline when appropriate. Obviously, reporting up the chain of command is preferable; but often that approach is problematic for one reason or another. So the company hotline is the best next option.

-

Let employees know that it's okay to use the hotline; that they will not be retaliated against. Rather, they will be protected.

-

Let employees know that their concerns will be taken seriously and that the concerns will be investigated impartially, perhaps by an outside party.

-

Let employees know that they will be hearing back from somebody with the results of those investigations.

-

Make sure that the company hotline number is prominently posted. Make it easy to dial. Make sure reports are logged.

Because the alternatives are much less pleasant.