

If you are not a government contractor and you want to become one, well, it's not an easy thing to do. We're not even talking about understanding the myriad rules and regulations that apply to government contractors, in which the violation of any one can crater your company. We (Apogee Consulting, Inc.) created a checklist to help companies new to government contracting understand those rules and regulations, which we use to evaluate contracting readiness. But that's not the first barrier to market entry you need to overcome.

No; understanding the rules of the game is not the first impediment you face. Before you can even play the game, you've got to register to play.

Before you even think about bidding on your first government contract, you need to register in several government databases. For example, you need a DUNS number from Dun & Bradstreet. You to register in the SAM (System for Award Management) database, which includes providing detailed information and executing some representations and certifications. At the end of the SAM registration process, you will get a CAGE number. You will probably want to register in the Small Business Administration's Dynamic Small Business Search (DSBS) database. In addition, many Federal agencies with whom you will want to do business have their own supplier databases, and you will want to register with those. In some cases, you may have to renew or update your registration annually.

There are many databases and each one wants detailed information and you have to provide that information if you want to play the Federal contracting game. Typically, the security of your information is provided by a User ID and a password, which you specify. As with all such security features, if you don't choose a strong password, you aren't doing yourself any favors. Further, if you don't protect that password, it doesn't matter how strong it is.

(We are reminded of one client who paid us to register his company into several government databases, which we did. But he never changed the passwords we initially used, despite our urging to do so. Some clients are challenging.)

Today's article is about fraud in the SAM system. In late March, 2018, the General Services Administration (GSA), the agency that manages SAM, [notified](#) contractors that "a third-party changed the financial information of 'a limited number' of contractors" in the SAM database. Apparently that third party entered SAM and changed the bank account information that the

SAM Fraud

Written by Nick Sanders
Friday, 27 April 2018 00:00

contractors had provided. Nobody knows exactly how this exploit was accomplished, but security experts stated the most likely approach was to obtain SAM passwords via a “phishing” attack. In any case, it was possible that if the government made payments to those contractors, the payments would end up in the wrong bank account. This is exactly what happened in 2016, when Dwayne Hans diverted \$1.5 million in PBGC payments to his own bank account. (Hans pleaded guilty and is currently awaiting sentencing as this article is being written.) SAM is no stranger to fraud. As Jason Miller’s story on Federal News Radio (link above) pointed out, “This is at least the third time SAM.gov has struggled to keep its information secure.”

Mr. Miller continues to [update](#) the story on the Federal News Radio website. In the latest update, he reported that “Up to 70,000 federal contractors are heading to their local notary to get that special stamp on a letter that’s destined for the General Services Administration to authenticate the vital details of their business, including who is the authorized ‘entity administrator associated with the DUNS number.’” According to the story, “GSA is requiring notarized letters for several thousand contractors immediately, and then any vendor whose existing registrations on SAM.gov need to be updated after April 27.”

At least 33,000 SAM registrants need to provide notarized confirmation that they intended to change their bank account information. The likelihood is that many of those registrants were intended victims of fraud. The problem is that many of those registrants are having challenges submitting the required notarized paperwork back to GSA. As Mr. Miller reported, “Of the 7,500 notarized letters received, GSA processed more than 3,300 and rejected almost 56 percent of them (1,910) for one reason or another.” That’s not a good statistic, is it?

SAM fraud. It should give every government contractor a chill. SAM registration is mandatory. If the sensitive information you enter isn’t secure, then the consequences for your company could be catastrophic.

On the other hand, cybersecurity is an important element of every online interaction. We reported [here](#) about recent attempts to hack our website. We have *not* reported about DFARS changes intended to make contractors secure “covered defense information.” (See DFARS 252.204-7012.) Why haven’t we addressed the cybersecurity compliance rules? Perhaps because law firms seem to have this one covered. For example: check [this summary](#) out. Or see one of the many articles authored by Bob Metzger of the firm Rogers Joseph O’Donnell.

SAM Fraud

Written by Nick Sanders
Friday, 27 April 2018 00:00

Even though we haven't made a big deal about it, cybersecurity is an extremely important topic, not only for government contractors, but for the government itself. As the recent SAM fraud demonstrates.