Is NSA Becoming Too Intrusive in Efforts to Stop Cyber-Crime?

July 13, 2010

The *Wall Street Journal* has just reported that the National Security Agency is planning to deploy electronic "sensors" in the private computer networks of major companies around the nation. The idea is to detect cyber-attacks by outside forces against companies involved in critical infrastructure like electric or nuclear plants.

Cyber-terrorism is a real threat, and the NSA is the only government agency, probably the only entity of any sort in the nation, that is truly equipped to monitor it. According to the article, national security officials are concerned about possible Chinese and Russian surveillance of our crucial computer networks.

However, the "Big Brother" aspect of this program is inescapable. Like many such programs, it began with a piecemeal effort and with the establishment by the government of co-operative relationships with private industry. But where will the program end? Conceivably, the government will soon routinely gain access to the private data of dozens of companies. Although it will surely pledge not to misuse this information, these pledges can't always be trusted.

And the article notes that while the government can't force any company to permit "sensors" to be introduced, it "can provide incentives to urge them to cooperate, particularly if the government already buys services from that company." That would include pretty much every government contractor – or in other words, every major company.

A few days ago, we noted in this blog that the FBI is now investigating possible instances of white-collar crime by deploying its massive electronic surveillance capacity.

Now, with the NSA's involvement in cyber-defense, we are again seeing the tentacles of government in the private sector, in the name of a good cause. This is troubling indeed.

Crime in the Suites is authored by the Ifrah Law Firm, a Washington DC-based law firm specializing in the defense of government investigations and litigation. Our client base spans many regulated industries, particularly e-business, e-commerce, government contracts, gaming and healthcare.

The commentary and cases included in this blog are contributed by Jeff Ifrah and firm associates Rachel Hirsch, Jeff Hamlin, Steven Eichorn and Sarah Coffey. These posts are edited by Jeff Ifrah and Jonathan Groner, the former managing editor of the Legal Times. We look forward to hearing your thoughts and comments!