# IF ONLY THEY HAD LISTENED TO THOMAS DRAKE, THEY MIGHT HAVE PREVENTED CABLEGATE

I'm in the process of reading all the Siobhan Gorman stories for which Thomas Drake might have served as an anonymous source. And one of the ten or so articles for which he's a possible source exposes the NSA's failure on an issue at the heart of Bradley Manning's ability to allegedly leak three major databases to WikiLeaks: adequate user authentication on the network.

The Drake indictment claims that Thomas Drake served as a source for "many" of the Siobhan Gorman articles she wrote about NSA between February 27, 2006 and November 28, 2007.

> Thereafter, between on or about February 27, 2006 and on or about November 28, 2007, Reporter A published a series of newspaper articles about NSA, including articles that contained SIGINT information. Defendant DRAKE served as a source for many of these newspaper articles, including articles that contained SIGINT information.

One of her articles from that period, published July 2, 2006, describes how the delay in implementing a new encryption management system for NSA and DOD computers exposed those networks to hackers.

> A National Security Agency program to protect secrets at the Defense Department and intelligence and other agencies is seven years behind schedule, triggering concerns that the data will be increasingly vulnerable to theft,

> according to intelligence officials and unclassified internal NSA documents obtained by The Sun.
>
> [snip]
>
> Encryption, which is an electronic lock, is among the most important of security tools, scrambling sensitive information so that it can ride securely in communications over the Internet or phone lines, and requiring a key to decipher.
>
> Powerful encryption is necessary for protecting information that is beamed from soldiers on the battlefield or that guards data in computers at the NSA's Fort Meade headquarters.

One of the three big things DOD claims it is doing to respond to WikiLeaks is to introduce smart cards for user credentials on SIPRNet.

> DoD has begun to issue a Public Key Infrastructure (PKI)-based identity credential on a hardened smart card. This is very similar to the Common Access Card (CAC) we use on our unclassified network. We will complete issuing 500,000 cards to our SIPRNet users, along with card readers and software, by the end of 2012. This will provide very strong identification of the person accessing the network and requesting data. It will both deter bad behavior and require absolute identification of who is accessing data and managing that access.
>
> In conjunction with this, all DoD organizations will configure their SIPRNet-based systems to use the PKI credentials to strongly authenticate end-users who are accessing information in the system. This provides the link between end users and the specific data they can access – not just network

> access. This should, based on our experience on the unclassified networks, be straightforward.

Which is precisely the kind of challenge one of Gorman's named sources in the article addresses.

> And as the demand grows for "smart" identification cards with computer chips that verify the card holder's identity, so does the need for sophisticated ways to manage who is being assigned cards, so that the cards do not end up in the wrong hands, said Stephen Kent, a chief scientist at BBN Technologies who has chaired government panels on information security.

Now, we have no way of knowing whether Drake was one of the 18 sources Gorman used for the article. But a number of her sources seem to compare this clusterfuck with that of Trailblazer—the program Drake and others submitted an Inspector General's complaint on.

> Like other major NSA efforts — such as the failed Trailblazer program to rapidly sift out threat information, and the troubled Groundbreaker program aimed at upgrading the agency's computer networks — an ever-changing game plan has caused many of the project's problems, current and former senior intelligence officials said.

Following that passage, Gorman cites a "former senior intelligence official"—the description (the indictment alleges) Drake asked Gorman to use when she cited him.

> One former senior intelligence official said that the NSA had unrealistic expectations from the start and repeatedly opted for delays to try to perfect the program. That left the government with aging security

> protections in the quest for security nirvana, the official said.
>
> "NSA often will say, `Well, this is not totally secure, so you can't use it,' when the only alternative is nothing," the former official said. "My worry is this push for perfect security is the enemy of good security.

And managing the implementation of a new key system sure sounds like something that the "Senior Change Leader" of NSA might be involved with.

Interestingly, the initial deadlines predicted in Gorman's article—2012—seem to roughly match the deadlines DOD now gives for its smart cards (as well as the insider threat detection, the deadline for which Obama is trying to push back further, though that may be a different issue).

Again, all that's not proof that Thomas Drake was warning in 2006 that if NSA didn't fix its management problems, something like CableGate would happen (as well as the widespread hacking we know to be happening).

But 18 people were warning of it back in 2006.

Which is, I guess, DOJ feels the need to prosecute whistleblowers, to cover up embarrassing lapses like this.