CHOKING THE SECURITY STATE WITH ITS OWN BOTTLENECK

One former and one current high-ranking intelligence official (is that you Keith?) have gone to CNBC to complain that tech firms are showing reluctance to get more of their people security clearances.

> U.S. government officials say privately they are frustrated that Silicon Valley technology firms are not obtaining U.S. security clearances for enough of their top executives, according to interviews with officials and executives in Washington and California. Those clearances would allow the government to talk freely with executives in a timely manner about intelligence they receive, hopefully helping to thwart the spread of a hack, or other security issues.
>
> The lack of cooperation from Silicon Valley, Washington officials complain, injects friction into a process that everyone agrees is central to the fight to protect critical U.S. cyberinfrastructure: Real-time threat information sharing between government and the private sector.
>
> [snip]
>
> The former intelligence official said dealing with Silicon Valley firms is much different than his experience in other industries—or with all American companies a generation ago. “It used to be, during World War II or the Cold War, that getting cooperation from boards of directors was pretty straightforward. That’s not true today, particularly at these huge start-ups that went from nothing to billions.”

It's interesting that this complainer went to CNBC's Eamon Javers, who covers the overlap between corporations and intelligence, rather than someone like Kim Zetter or Shane Harris, who just finished interesting books on cybersecurity. Because the only challenge to those DC insiders' claims about the importance of information sharing comes from this anonymous executive's suggestion that the intelligence they'd get from the government isn't all that useful.

> In Silicon Valley, however, cybersecurity executives have a different perspective on the tension. "I believe that this is more about the overclassification of information and the relatively low value that government cyberintel has for tech firms," said one Silicon Valley executive. "Clearances are a pain to get, despite what government people think. Filling out the paper work … is a nightmare, and the investigation takes a ridiculous amount of time."

More generally (including in each of their books), I think people are raising more questions about the value of information sharing. At a recent panel on cybersecurity (starting at 12:20) for example, a bunch of security experts seemed to agree that information sharing shouldn't be the priority it is. Yahoo CISO Alex Stamos (who at the same conference had this awesome exchange with NSA Director Mike Rogers) argued that the government emphasizes information sharing because it's easy — he'd rather see the government cancel just one F-35 and put the money into bug bounties for open source software.

Nevertheless, these sources have been granted anonymity to suggest tech companies are un-American because they're not rushing to share more data with the federal government.

Not to mention, not rushing to sign up to have

their lives regulated by the McCarthyite system of security clearances.

Because it’s not just that the security clearance application that is unwieldy. It’s that clearance comes with a gag order about certain issues, backed by the threat of prison (I forget whether it was Harris’ or Zetter’s book, but one describes a tech expert talking about that aspect of clearance).

Why would anyone sign up for that if the tech companies have more that the government wants than the government has that the tech companies need?

So it will be interesting to see how the security establishment respond to this. It would be a wonderful way to force the government fix some of the problems with overclassification to be able to obtain the cooperation of what are supposed to be private corporations.